Spring 2020

Two Inquiries Related to the Digits of Prime Numbers

Jeremiah T. Southwick

Two inquiries related to the digits of prime numbers

by

Jeremiah T. Southwick

Bachelor of Arts
Le Moyne College, 2014

Master of Arts
Wake Forest University, 2016

Submitted in Partial Fulfillment of the Requirements

for the Degree of Doctor of Philosophy in

Mathematics

College of Arts and Sciences

University of South Carolina

2020

Accepted by:

Michael Filaseta, Major Professor

Matthew Boylan, Committee Member

Maria Girardi, Committee Member

Ognian Trifonov, Committee Member

Karl Gregory, Committee Member

Cheryl L. Addy, Vice Provost and Dean of the Graduate School

Dedication

To each of the individuals who helped develop my love and appreciation for the beauty of math.

To my parents. My mother served as my teacher in grade school and made sure I arrived in college with a sound educational backing, day in and day out, year in and year out. My father helped me with the math topics that were beyond mom's expertise, and dad's job as a math teacher was my initial inspiration for pursuing a degree in mathematics.

To Jonathan Needleman, who found an incredibly compelling research problem for me to work on for my undergraduate thesis and who kindled my original interest in number theory with an elementary number theory class taught via the Moore method.

To Sarah Mason, who introduced me to combinatorial game theory and who helped me see the value in counting things.

To Michael Filaseta, who always has the simplest proofs for the most surprising theorems and who through several iterations over four years of homework assignments, exams, papers, and this dissertation, has helped me polish up the way I talk about math and share it with others.

Acknowledgments

The work in this dissertation is mine in the sense that I worked on formulating, establishing, and carefully writing up the results. But in another sense, the work that follows was a joint effort of many individuals. Thanks are owed first and foremost to Michael Filaseta, for agreeing to work with me and for suggesting the several research projects appearing in this dissertation. His insights into each topic, often several steps ahead of mine, kept things moving forward and allowed me to proceed at the pace I did.

I also owe thanks to Joseph Foster and Jacob Juillerat. I was only able to survive my qualifying and comprehensive exams because I had them to study with. Eventually we became coauthors and muddled through our first paper together, critiquing and complementing our way initially to a mathematically valid paper and then finally to a moderately well-written article. In all our research together, they were invaluable as honest, enthusiastic minds to bounce ideas off of and with which to share the struggles and successes of research.

No list of thanks would be complete without acknowledging my wife Jacqueline, who has been a constant encouragement in my studies. We began marriage at the same time I started my PhD program, and while those were not the most auspicious conditions to begin the joy of our lifelong commitment to each other, she has been remarkable in her dedication to making sure I complete the program successfully. She simultaneously provided a structure and surety to my time outside of mathematics that has enriched my life and our relationship in innumerable ways. I am blessed to be married to a woman as thorough, sharp, and excellent as Jacqueline.

Abstract

This dissertation considers two different topics. In the first part of the dissertation, we show that a positive proportion of the primes have the property that if any one of their digits in base 10, including their infinitely many leading 0 digits, is replaced by a different digit, then the resulting number is composite. We show that the same result holds for bases $b \in \{2, 3, \cdots, 8, 9, 11, 31\}$.

In the second part of the dissertation, we show for an integer $b \geq 5$ that if a polynomial $f(x)$ with non-negative coefficients satisfies the condition that $f(b)$ is prime, there are explicit bounds $D_4(b)$ and $D_3(b)$ so that if the degree of $f(x)$ is $\leq D_4$, then $f(x)$ is irreducible; and if the degree of $f(x)$ is $\leq D_3$ and $f(x)$ is reducible, then $f(x)$ is divisible by the shifted cyclotomic polynomial $\Phi_4(x-b)$. Furthermore, in the case that $b > 26$, there are explicit bounds $D_6(b)$ and $D(b)$ so that if the degree of $f(x)$ is $\leq D_6$ and $f(x)$ is reducible, then $f(x)$ is divisible by either $\Phi_4(x-b)$ or $\Phi_3(x-b)$; and if the degree of $f(x)$ is $\leq D$ and $f(x)$ is reducible, then $f(x)$ is divisible by $\Phi_4(x-b)$, $\Phi_3(x-b)$, or $\Phi_3(x-b)$. Furthermore, we show that for each $b \geq 5$ and each $n \in \{3, 4, 6\}$, the bound D_n is sharp.

Table of Contents

Dedication iii

Acknowledgments iv

Abstract v

List of Tables viii

List of Figures xi

Chapter 1 Introduction 1

1.1 Results pertaining to changing the digits of a number 1

1.2 Results pertaining to polynomial irreducibility 6

1.3 Other results 9

Chapter 2 Widely Digitally Delicate Primes 12

2.1 Increasing a digit 12

2.2 Decreasing a digit 25

2.3 Related topics and open problems 29

Chapter 3 Irreducibility criteria based on degree for polynomials with non-negative coefficients 35

3.1 Preliminary results 35

3.2 A root bounding function 36

3.3 Irreducibility criteria based on degree 41

Bibliography 55

Appendix A Coverings for bases other than 10 58

A.1 Covering systems for $b = 2$ 59

A.2 Covering systems for $b = 3$ 59

A.3 Covering systems for $b = 4$ 60

A.4 Covering systems for $b = 5$ 61

A.5 Covering systems for $b = 6$ 61

A.6 Covering systems for $b = 7$ 63

A.7 Covering systems for $b = 8$ 65

A.8 Covering systems for $b = 9$ 68

A.9 Covering systems for $b = 11$ 69

A.10 Covering systems for $b = 31$ 70

Appendix B SageMath code 86

B.1 Finding prime divisors of $\Phi_n(a)$ 86

B.2 Checking whether primes are digitally delicate 88

B.3 Checking whether a system of congruences is a covering 92

List of Tables

Table 2.1 Covering used in Lemma 2.2 (i) for $A + 4 \cdot 10^k$ 17

Table 2.2 Covering used in Lemma 2.2 (i) for $A + 1 \cdot 10^k$ 18

Table 2.3 Covering used in Lemma 2.2 (i) for $A + 6 \cdot 10^k$ 18

Table 2.4 Covering used in Lemma 2.2 (i) for $A + 9 \cdot 10^k$ 19

Table 2.5 Partial factorizations of $\Phi_n(10)$ for large n 21

Table 2.6 First part of covering used for $A + 3 \cdot 10^k$ 22

Table 2.7 Second part of covering used for $A + 3 \cdot 10^k$ 23

Table 2.8 Third part of covering used for $A + 3 \cdot 10^k$ 24

Table 2.9 $\mathcal{L}_b(k, \ell)$ for bases $b \in \{2, 3, \cdots, 10\}$ 30

Table A.1 Covering for $A + 1 \cdot 2^k$ 59

Table A.2 Covering for $A + 2 \cdot 3^k$ 60

Table A.3 Covering for $A + 2 \cdot 4^k$ 60

Table A.4 Covering for $A + 3 \cdot 4^k$ 60

Table A.5 Covering for $A + 4 \cdot 5^k$ 61

Table A.6 Covering for $A + 2 \cdot 5^k$ 61

Table A.7 Covering for $A + 1 \cdot 6^k$ 62

Table A.8 Covering for $A + 2 \cdot 6^k$ 62

Table A.9 Covering for $A + 4 \cdot 6^k$ 62

Table A.10 Covering for $A + 5 \cdot 6^k$ 63

Table A.11 Covering for $A + 4 \cdot 7^k$ 64

Table A.12 Covering for $A + 6 \cdot 7^k$ 64

Table A.13 Covering for $A + 1 \cdot 8^k$ 65

Table A.14 Covering for $A + 2 \cdot 8^k$ 65

Table A.15 Covering for $A + 4 \cdot 8^k$ 65

Table A.16 Covering for $A + 5 \cdot 8^k$ 65

Table A.17 Covering for $A + 6 \cdot 8^k$ 66

Table A.18 Partial factorizations of $\Phi_n(8)$ for large n 66

Table A.19 First part of covering for $A + 7 \cdot 8^k$ 66

Table A.20 Second part of covering for $A + 7 \cdot 8^k$ 67

Table A.21 Covering for $A + 6 \cdot 9^k$ 68

Table A.22 Covering for $A + 2 \cdot 9^k$ 68

Table A.23 Covering for $A + 4 \cdot 9^k$ 68

Table A.24 Covering for $A + 8 \cdot 9^k$ 69

Table A.25 Covering for $A + 4 \cdot 11^k$ 69

Table A.26 Covering for $A + 10 \cdot 11^k$ 70

Table A.27 Covering for $A + 8 \cdot 11^k$ 70

Table A.28 Covering for $A + 6 \cdot 11^k$ 70

Table A.29 Covering for $A + 26 \cdot 31^k$ 71

Table A.30 Covering for $A + 30 \cdot 31^k$ 72

Table A.31 Partial factorizations of $\Phi_n(31)$ for large n 73

Table A.32 More partial factorizations of $\Phi_n(31)$ for large n 74

Table A.33 Complete factorizations of $\Phi_n(31)$ for large n 74

Table A.34 Covering for $A + 8 \cdot 31^k$ 74

Table A.35 First part of covering for $A + 2 \cdot 31^k$ 75

Table A.36 Second part of covering for $A + 2 \cdot 31^k$ 76

Table A.37 Third part of covering for $A + 2 \cdot 31^k$ 77

Table A.38 Covering for $A + 6 \cdot 31^k$ 78

Table A.39 First part of covering for $A + 12 \cdot 31^k$ 79

Table A.40 Second part of covering for $A + 12 \cdot 31^k$ 80

Table A.41 First part of covering for $A + 18 \cdot 31^k$ 80

Table A.42 Second part of covering for $A + 18 \cdot 31^k$ 81

Table A.43 Third part of covering for $A + 18 \cdot 31^k$ 82

Table A.44 Fourth part of covering for $A + 18 \cdot 31^k$ 83

Table A.45 First part of covering for $A + 20 \cdot 31^k$ 84

Table A.46 Second part of covering for $A + 20 \cdot 31^k$ 85

List of Figures

Figure 3.1 L_5 together with $\mathcal{R}_5$ 45

Chapter 1

Introduction

In this dissertation, we detail a variety of number theoretic results. Broadly speaking, these results fall into either the topic of digit changing or that of polynomial irreducibility. The results in this introduction are therefore split into two sections depending on which topic they pertain to, and the proofs that follow in the dissertation are split into two chapters based on the same criterion. A third section of the introduction lists several results which the author helped to establish, the proofs of which appear in other dissertations.

1.1 Results pertaining to changing the digits of a number

In 1978, M. S. Klamkin [19] proposed the following problem: Does there exist any prime number such that if any digit (in base 10) is changed to any other digit, the resulting number is always composite? Shortly afterwards, P. Erdős [5] provided a proof that there are an infinite number of such primes. The first several are

$$294001, \quad 505447, \quad 584141, \quad 604171, \quad 971767, \quad 1062599,$$
$$1282529, \quad 1524181, \quad 2017963, \quad 2474431, \quad 2690201, \quad 3085553.$$

A complete list up to 10^9 can be found through a link in [26]. More recently, T. Tao [30] established that a positive proportion of the primes satisfy the conditions in Klamkin's problem, and J. Hopper and P. Pollack [17] showed that a positive proportion of the primes become composite if one modifies any single digit and appends a bounded number of digits at the beginning or end. To clarify, following the wording

of J. Hopper and P. Pollack [17], we define a prime p as being *digitally delicate* if it has the property given in Klamkin's problem, that is, if any one of its digits is changed, then the resulting number is composite. If $\pi_d(x)$ denotes the number of digitally delicate primes up to x and, as usual, $\pi(x)$ denotes the number of primes up to x, then Tao's work implies

$$\liminf_{x\to\infty} \frac{\pi_d(x)}{\pi(x)} > 0.$$

As

$$\frac{\pi_d\Big(10^{10}\Big)}{\pi\Big(10^{10}\Big)} = \frac{32323}{455052511} = 0.000071031\ldots,$$

it seems likely the liminf above is very small.

The work of Erdős can be generalized to any base, and Tao as well as Hopper and Pollack gave rather general results for arbitrary bases. For example, note that a prime p in base b has $r = r(p,b) = \lfloor \log_b p \rfloor + 1$ base b digits. Thus, we can write a prime p in base b as $\sum_{j=0}^{r-1} d_j b^j$ where $0 \le d_j \le b-1$ for each j. Tao's work allows one to extend Klamkin's problem by including a number of leading 0's in the prime p. Taking $s > r$, we can write

$$p = \sum_{j=0}^{s} d_j b^j, \quad \text{where} \quad d_j = \begin{cases} 0 & \text{if } j \ge r \\ \text{some number in } \{0,1,\ldots,b-1\} & \text{if } 0 \le j < r. \end{cases}$$

Hence, we can view p as having $> r$ digits by allowing leading 0's.

Theorem 1.1 (Tao)**.** *For every integer $C > 0$, a positive proportion of the primes p have the property that in every base $b \in [2, C]$ if any of the $C\Big(\lfloor \log_b(p) \rfloor + 1\Big)$ base b digits of p, including $(C-1)\Big(\lfloor \log_b(p) \rfloor + 1\Big)$ leading 0's, is changed to another digit, then the the resulting number is composite.*

As an interesting related example, the first prime in base 10 for which the number of leading 0's that can be included in Klamkin's problem is greater than the number

of digits of the prime is the prime $p = 354975121$. The smallest prime that occurs by changing any one digit of p including leading 0's is

$$70000000000354975121.$$

In this dissertation, we consider primes with leading 0's on a larger scale.

Definition 1.2. A *widely digitally delicate* prime is a prime with the property that if any one of its digits, including any of its infinitely many leading 0's, is replaced by any different digit, then the resulting number is composite.

While this notion makes sense in any base, we will focus in Chapter 2 on widely digitally delicate primes in base 10. We establish the following theorem about such primes.

Theorem 1.3. *A positive proportion of the primes in base 10 are widely digitally delicate.*

We do not know of any examples of widely digitally delicate primes in base 10. None of the digitally delicate primes up to 10^9 listed through [26] are widely digitally delicate.

We prove Theorem 1.3 in Sections 2.1 and 2.2. In Section 2.1, we exhibit specific covering systems in a manner similar to [10] to show that for sufficiently large primes p satisfying a certain congruence, increasing any digit (possibly a leading 0) in the base 10 expansion of p results in a composite number. In Section 2.2, we first use a partial covering similar to the argument of Erdős in [5] to show that for p satisfying a second congruence, most changes arising from decreasing a digit of p result in a composite number. We then mimic Tao's argument in [30] by using a sieve to show that many of these primes become composite when one of the few remaining nonzero digits is decreased, so that Theorem 1.3 follows.

Because our argument depends on exhibiting particular covering systems which allow for increasing a digit in base 10, our proof does not generalize directly to other bases. However, the rest of our argument only depends on the existence of such a covering system, so to prove the statement analogous to Theorem 1.3 for a given base b it suffices to exhibit a covering system which establishes that any increase of a digit in base b results in a composite number. We have found such covering systems for bases $b \in \{2, 3, \ldots, 11\}$, which are listed in Appendix A. However, our methods become difficult to replicate as b grows. We also looked at the base $b = 31$ since finding a covering is simplified in the case that $b - 1$ has distinct small prime factors. We were able to show that a positive proportion of the primes are widely digitally delicate in base 31, and the coverings for that argument also appear in Appendix A. We emphasize again though that we do not know whether a result similar to Theorem 1.3 holds for an arbitrary base.

The corresponding case of $b = 2$ in Theorem 1.3 has received prior attention in the literature in a different form. The theorem in this case is connected to a number being both a Sierpiński and a Riesel number. A Sierpiński number is a number n such that $n \cdot 2^k + 1$ is composite for all non-negative integers k, and a Riesel number is a number n such that $n \cdot 2^k - 1$ is composite for all non-negative integers k. D. Ismailescu and P. S. Park [18] have shown that if

$$n \equiv 10439679896374780276373 \pmod{6648308496158851012401069159 0},$$

then n is both a Sierpiński and a Riesel number.

The notion of a Sierpiński prime relates to the notion of a widely digitally delicate prime in the following way: Let $n \in \mathbb{Z}^+$. One can show, as was shown for Riesel numbers in Lemma 4 of [8], that if there is a finite set of primes $\mathcal{P}$ so that for all sufficiently large k, some prime $p \in \mathcal{P}$ divides $n \cdot 2^k + 1$ (respectively $n \cdot 2^k - 1$), then for all k in $\mathbb{Z}$, the number $n + 2^k$ (respectively $n - 2^k$) is divisible by some prime $p \in \mathcal{P}$. Since the proof in [18] which obtained the congruence above relied on determining

such a set $\mathcal{P}$ for each of the numbers $n \cdot 2^k + 1$ and $n \cdot 2^k - 1$ where k is a non-negative integer, and since the set $\mathcal{P}$ has elements less than any element of

$$\left\{ |1043967989637478027637 3 \pm 2^k| \ : \ k \in \mathbb{Z}^+ \cup \{0\} \right\},$$

it follows that primes p satisfying this congruence and, hence, a positive proportion of primes, satisfy that $p + 2^k$ and $p - 2^k$ are composite for every non-negative integer k. In particular, the prime

$$10439679896374780276373$$

has the property that if any of its base 2 digits, including any of its infinitely many leading 0's, is replaced by a different digit, then the resulting number is composite.

The smallest proven widely digitally delicate prime in base 2 is 2131099, which we obtained by looking for digitally delicate Sierpiński primes. We searched the numbers listed through [27] for digitally delicate primes and 2131099 was the smallest such prime. It is widely digitally delicate since 2131099 is digitally delicate and has been proven to be a Sierpiński number with covering set

$$\mathcal{P} = \{3, 5, 7, 13, 17, 241\},$$

so that the numbers $2131099 + 2^k$ are also composite for all non-negative integers k since any base 2 digit change in 2131099 results in a number larger than 241.

We have also used the coverings listed in Appendix A to find a prime which is widely digitally delicate in base 3. Beyond this, we have been unable to find widely digitally delicate primes in other bases.

There are a number of interesting open questions related to Theorem 1.3 that can be asked, which we address in Section 2.3.

1.2 Results pertaining to polynomial irreducibility

If $d_n d_{n-1} ... d_1 d_0$ is the decimal representation of a prime, then a result of A. Cohn [22] asserts that

$$f(x) = d_n x^n + d_{n-1} x^{n-1} + \cdots + d_1 x + d_0$$

is irreducible over the integers. This result can be generalized in several directions if we view $f(x)$ as a polynomial with non-negative coefficients and $f(10)$ prime. Questions arise in this setting: Does the irreducibility of $f(x)$ depend on the coefficients being less than 10? Can we find a degree n so that if $f(x)$ has degree less than n, then $f(x)$ is irreducible? Is 10 special, or do similar results hold when we replace the condition that $f(10)$ is prime with the condition that $f(b)$ is prime for some positive integer $b \neq 10$?

Various answers to these questions can be found in the literature. The result of Cohn has been extended to all bases $b \geq 2$ by J. Brillhart, A. Odlyzko and M. Filaseta [2]. In [6], M. Filaseta extended this to base b representations of kp where k is a positive integer $< b$ and p is a prime, and M. R. Murty [23] has an analog in function fields over finite fields. Furthermore, [2] allows the coefficients d_j in Cohn's theorem to satisfy $0 \leq d_j \leq 167$ rather than $0 \leq d_j \leq 9$; and later M. Filaseta [7] showed that the d_j need only satisfy $0 \leq d_j \leq 10^{30} d_n$, and further that simply $d_j \geq 0$ suffices if $n \leq 31$.

More recently, work by S. Gross and M. Filaseta [9] extended this line of investigation in other ways. They showed that if $f(x)$ is a polynomial with non-negative coefficients, $f(10)$ prime, and the degree of $f(x)$ less than or equal to 34, then $f(x)$ is reducible only in the case that $f(x)$ is divisible by $\Phi_4(x-10) = x^2 - 20x + 101$, where $\Phi_n(x)$ is the nth cyclotomic polynomial. They further showed that if 34 is instead replaced by 36, then $f(x)$ is reducible only if it is divisible by one of $\Phi_4(x-10)$ and $\Phi_3(x-10)$.

Building on this work in [4], M. Cole, S. Dunn, and M. Filaseta extended this result in the setting where $f(b)$ is prime, $2 \leq b \leq 20$, to find similar bounds $D(b)$, $D_1(b)$, and $D_2(b)$ so that if the degree of $f(x)$ is less than or equal to $D(b)$, then $f(x)$ is irreducible, if the degree of $f(x)$ is less than or equal to $D_1(b)$ and $f(x)$ is reducible, then $\Phi_4(x-b)$ divides $f(x)$, and if the degree of $f(x)$ is less than or equal to $D_2(b)$ and $f(x)$ is reducible, then $f(x)$ is divisible by $\Phi_4(x-b)$ or $\Phi_3(x-b)$. Our main goal for this section of the dissertation will be to extend these results via the theorem below. Note that we have modified the notation used from that in [4].

Theorem 1.4. *Fix an integer $b \geq 5$, and for $n \in \{3,4,6\}$ set*

$$D_n = D_n(b) = \left\lfloor \frac{\pi}{\arg(b+\zeta_n)} \right\rfloor \qquad \text{and} \qquad D = D(b) = \left\lfloor \frac{\pi}{\arctan\left(\frac{1732}{1000(2b+1)}\right)} \right\rfloor.$$

Let $f(x) \in Z[x]$ with non-negative coefficients and with $f(b)$ prime. If the degree of $f(x)$ is $\leq D_4$, then $f(x)$ is irreducible. Additionally, if the degree of $f(x)$ is $\leq D_3$ and $f(x)$ is reducible, then $f(x)$ is divisible by $\Phi_4(x-b)$ and not divisible by $\Phi_3(x-b)$ or $\Phi_6(x-b)$. Furthermore, in the case that $b > 26$, if the degree of $f(x)$ is $\leq D_6$ and $f(x)$ is reducible, then $f(x)$ is divisible by either $\Phi_4(x-b)$ or $\Phi_3(x-b)$ and not by $\Phi_6(x-b)$. Lastly, in the case that $b > 26$, if the degree of $f(x)$ is $\leq D$ and $f(x)$ is reducible, then $f(x)$ is divisible by $\Phi_4(x-b)$, $\Phi_3(x-b)$, or $\Phi_3(x-b)$.

The proof of Theorem 1.4, which appears in Chapter 3, relies heavily on the techniques established in both [9] and [4]. Throughout the dissertation, irreducibility will refer to irreducibility in $\mathbb{Z}[x]$. We show in Chapter 3 that the bounds $D_n(b)$ above are sharp, in that they are the largest numbers having the stated property. However, we do not know if $D(b)$ is sharp. In particular, the denominator in the floor in D corresponds to an approximation of

$$\arctan\left(\frac{\sqrt{3}}{2b+1}\right).$$

As b grows, one can allow for less precise approximations of $\sqrt{3}$ in D which admit the same results as those in Theorem 1.4.

On the coefficient side of this question, it was shown in [9] that if $f(x)$ is a polynomial with non-negative coefficients bounded above by

$$495986669891512260981042445129 18$$

and $f(10)$ is prime, then $f(x)$ is irreducible over $\mathbb{Z}$. S. Gross and M. Filaseta also showed that if the coefficients were instead bounded above by

$$859244474352913581576954595593 6773,$$

then $f(x)$ is either irreducible over $\mathbb{Z}$ or divisible by $\Phi_4(x-b) = x^2 - 20x + 101$. Furthermore, they showed that these bounds are sharp, i.e., they exhibited polynomials with maximum coefficient one more than the numbers displayed above which were reducible (and in the second case, not divisible by $x^2 - 20x + 101$).

This work was generalized further in [4], which found bounds $M_1(b)$ such that if the coefficients of $f(x)$ are bounded above by $M_1(b)$, and $f(b)$ is prime for an integer $b \in [2, 20]$, then $f(x)$ is irreducible over $\mathbb{Z}$. They also found bounds $M_2(b)$ such that if the coefficients of $f(x)$ are bounded above by $M_2(b)$, and $f(b)$ is prime for $3 \le b \le 5$, then $f(x)$ is either reducible or divisible by $\Phi_3(x-b)$. Similarly, if $6 \le b \le 20$, and the coefficients of $f(x)$ are bounded above by $M_2(b)$, then $f(x)$ is either reducible or divisible by $\Phi_4(x-b)$. Furthermore, they established that the upper bounds $M_1(b)$ are sharp for $3 \le b \le 20$, and that the upper bounds $M_2(b)$ are sharp for $4 \le b \le 20$.

We state here an extension of the results in [4] to all integers $b \ge 2$.

Theorem 1.5. *Let $b \in \mathbb{Z}$ with $b > 2$ and let $n \in \{3, 4, 6\}$. Set*

$$D_n = D_n(b) = \left\lfloor \frac{\pi}{\arg(b + \zeta_n)} \right\rfloor.$$

Let $f(x) = \sum_{j=0}^{N} a_j x^j$ with $a_j \ge 0$ for each j and $f(b)$ prime. Let

$$\mathcal{B}_b^{(n)} = \max\left(\mathcal{B}_{b,1}^{(n)}, \mathcal{B}_{b,2}^{(n)}\right)$$

where

$$\mathcal{B}_{b,1}^{(n)} = \left(\sum_{0 \le k \le \frac{D_n}{2}} \binom{D_n}{2k+1} (b + \mathrm{Re}(\zeta_n))^{D_n - 2k - 1} (-\mathrm{Im}(\zeta_n)^2)^k \right) (1 - A_n + B_n)$$

and

$$\mathcal{B}_{b,2}^{(n)} = \left(\sum_{0 \le k \le \frac{D_n - 1}{2}} \binom{D_n - 1}{2k+1} (b + \mathrm{Re}(\zeta_n))^{D_n - 2k - 2} (-\mathrm{Im}(\zeta_n)^2)^k \right) (1 - A_n + B_n), \tag{1.1}$$

for $(A_3, A_4, A_6) = (2b-1, 2b, 2b+1)$ *and* $(B_3, B_4, B_6) = (b^2 - b + 1, b^2 + 1, b^2 + b + 1)$. *Also, for* $b > 20$ *let*

$$\mathcal{B}_b = \frac{(b - 1.5221)^{k_b}(b - 2.5221)}{1 + \cot(\pi/b^2)} \quad \textit{with} \quad k_b = \left\lfloor \frac{(b^2 - 1)\pi}{b^2 \phi} \right\rfloor, \tag{1.2}$$

where $\phi = \arctan(0.8444/(b - 0.2))$, *and for* $2 \le b \le 20$ *define* $\mathcal{B}_b$ *to be values chosen in [22, Table 10]. Then the following hold.*

For $b = 2$, *if each* $a_j \le 7$, *then* $f(x)$ *is irreducible. For* $3 \le b \le 5$, *if each* $a_j \le \mathcal{B}_b^{(3)}$, *then* $f(x)$ *is irreducible. For* $b > 5$, *if each* $a_j \le \mathcal{B}_b^{(4)}$, *then* $f(x)$ *is irreducible. For* $3 \le b \le 5$, *if each* $a_j \le \mathcal{B}_b^{(4)}$ *and* $f(x)$ *is reducible, then* $f(x)$ *is divisible by* $\Phi_3(x - b)$. *For* $b > 5$, *if each* $a_j \le \mathcal{B}_b^{(3)}$ *and* $f(x)$ *is reducible, then* $f(x)$ *is divisible by* $\Phi_4(x - b)$. *For* $b > 69$, *if each* $a_j \le \mathcal{B}_b^{(6)}$ *and* $f(x)$ *is reducible, then* $f(x)$ *is divisible by* $\Phi_3(x - b)$ *or* $\Phi_4(x - b)$. *For* $b > 69$, *if each* $a_j \le \mathcal{B}_b$ *and* $f(x)$ *is reducible, then* $f(x)$ *is divisible by* $\Phi_3(x - b)$, $\Phi_4(x - b)$, *or* $\Phi_6(x - b)$.

The proof of Theorem 1.5 will be discussed further in the dissertations of J. Foster and J. Juillerat.

1.3 Other results

We now proceed to other results of the author. In [12], J. Foster, J. Juillerat, and the author use Newton polygons to establish that a certain family of polynomials is

irreducible. The work stems from [14], in which Heim, Luca and Neuhauser study the functions

$$\exp\left(x\sum_{n\geq 1} g(n)\frac{q^n}{n}\right) = \sum_{n\geq 0} P_n^g(x)q^n,$$

where $q = e^{2\pi i\tau}$ with τ in the upper complex half-plane, and $g : \mathbb{N} \to \mathbb{N}$ is an arithmetic function normalised such that $g(1) = 1$. Given these restraints, the polynomials $P_n^g(x)$ can be shown to satisfy the recursive relationship

$$P_n^g(x) = \frac{x}{n}\sum_{k=1}^{n} g(k)P_{n-k}^g(x)$$

for all $n \geq 1$, where $P_0^g(x) = 1$. Of particular interest in [14] is the case that $g(n) = \sigma(n) = \sum_{d|n} d$. In this setting, the roots of the polynomials $P_n^\sigma(x)$ appearing as coefficients in the resulting q-power series can be shown to dictate the vanishing properties of the nth Fourier coefficients of powers of the Dedekind eta function (see, for example, [16], [21]).

Using the fact that $n \leq \sigma(n) \leq n^2$, Heim, Luca and Neuhauser seek to gain information about $P_n^\sigma(x)$ and their roots by considering the family of polynomials $P_n^g(x)$ where $g(n) = n$ and $g(n) = n^2$.

In the case that $g(n) = n$, the recursive formula for $P_n^g(x)$ gives the closed form

$$P_n^g(x) = x\sum_{k=0}^{n-1}\binom{n-1}{k}\frac{x^k}{(k+1)!}.$$

Using a result of Schur [24] regarding the irreducibility of the generalized Laguerre polynomials, they show that in this case when $g(n) = n$ the polynomial $P_n^g(x)$ is x times an irreducible polynomial. However, this result does not apply when $g(n) = n^2$, in which case they show $P_n^g(x) = x\widetilde{P}_n(x)$ where

$$\widetilde{P}_n(x) = \sum_{j=0}^{n-1}\frac{1}{(j+1)!}\binom{n+j}{2j+1}x^j.$$

The polynomial $\widetilde{P}_n(x)$ is Eisenstein when $n-1$ is prime, and hence $\widetilde{P}_n(x)$ is irreducible. Heim, Luca, and Neuhauser leave as an open question whether the $\widetilde{P}_n(x)$

are irreducible for general n. Using Newton polygons, J. Foster, J. Juillerat, and the author establish the following theorem, which will be discussed further in the dissertations of J. Foster and J. Juillerat.

Theorem 1.6. *The polynomials $\widetilde{P}_n(x)$ are irreducible over $\mathbb{Q}$ for all positive integers n.*

Using methods similar to those established by Heim and Neuhauser in [15], J. Foster and the author have generalized Theorem 1.6 to hold when $g(n) = n^{t+1}$, $t \in \mathbb{Z}^+$. In this case, the polynomials $P_n^g(x)$ take the closed form

$$x \sum_{k=1}^{n} \frac{S(n|k,t)}{k!} x^{k-1}$$

where

$$S(n|k,t) = \sum_{m_1+\cdots+m_k=n} m_1^t \cdots m_k^t = [x^n] \left(\left(x + 2^t x^2 + 3^t x^3 + \cdots \right)^k \right)$$

and $[x^n](\cdot)$ denotes the nth coefficient operator. In the case that $t = 1$, $S(n|k,1)$ specializes to the binomial coefficient $\binom{n+j-1}{2j-1}$ appearing in $\widetilde{P}_n(x)$.

One can show that the formula for $S(n|k,t)$ above simplifies to the $(n-k)$th coefficient of x in the expansion

$$\left(\sum_{k_0+\cdots+k_{t-1}=k} \binom{k}{k_0,\ldots,k_{t-1}} \left(\prod_{i=0}^{t-1} A(t,i)^{k_i} \right) x^{\sum_{i=0}^{t-1} i k_i} \right) \sum_{j=0}^{\infty} \binom{j+(t+1)\,k-1}{(t+1)\,k-1} x^j,$$

where the numbers $A(t,i)$ are the so-called Eulerian numbers. Using this formula and an argument involving Newton polygons similar to that in [12], J. Foster and the author establish the following theorem.

Theorem 1.7. *Let $t \in \mathbb{Z}^+$ and let $g_t(n) = n^{t+1}$. Then the polynomial*

$$P_n^{g_t}(x) = x \sum_{k=1}^{n} \frac{S(n|k,t)}{k!} x^{k-1}$$

is x times an irreducible polynomial.

Chapter 2

Widely Digitally Delicate Primes

2.1 Increasing a digit

We remind the reader of the following definition and theorem from the introduction.

Definition 1.2. A *widely digitally delicate* prime is a prime with the property that if any one of its digits, including any of its infinitely many leading 0's, is replaced by any different digit, then the resulting number is composite.

Theorem 1.3. *A positive proportion of the primes in base 10 are widely digitally delicate.*

We begin by establishing that a positive proportion of primes p satisfy that the numbers $p + \delta \cdot 10^k$ are composite

$$\forall\, \delta \in \{1, 2, \ldots, 8, 9\} \quad \text{and} \quad \forall\, k \in \mathbb{Z}^+ \cup \{0\}.$$

This then will account for changing any leading 0 of p as well as increasing any digit of p that is not a leading 0. The approach here is similar to that used in [10]. We achieve the above by constructing finite sets of primes $\mathcal{P}_\delta$ which arise from constructing a covering (defined below) for the powers of k appearing in the numbers $p + \delta \cdot 10^k$. Then p will have the property we want if we choose p from an appropriate residue class A modulo the product of primes in $\mathcal{P}_1 \cup \mathcal{P}_2 \cup \cdots \cup \mathcal{P}_9$.

Definition 2.1. A finite system of congruences $x \equiv a_i \pmod{m_i}$, $1 \leq i \leq t$, is called a *covering of the integers* (or simply a *covering*) if each integer satisfies at least one congruence in the system.

For example, one can check that the system

$$\begin{aligned} x &\equiv 0 \pmod 2 \\ x &\equiv 1 \pmod 3 \\ x &\equiv 3 \pmod 4 \\ x &\equiv 5 \pmod 6 \\ x &\equiv 9 \pmod{12} \end{aligned}$$

is a covering of the integers. Although this example is a covering where the moduli are distinct, for our purposes, we do not want to require that the moduli need be distinct.

We next state and prove a simple lemma, similar to Lemma 1 in [10], which clarifies our use of covering systems. By way of notation, we use $c(p)$ to refer to the multiplicative order of 10 modulo a prime p with $\gcd(p, 10) = 1$.

Lemma 2.2. *Let $A \in \mathbb{Z}^+$. For a fixed $\delta \in \{0, \ldots, 9\}$, suppose we have distinct primes $p_1, \ldots, p_t$, each relatively prime to 10, satisfying the following.*

(i) There exists a covering of the integers

$$k \equiv b_i \pmod{c(p_i)}, \quad 1 \leq i \leq t.$$

(ii) The number A satisfies each of the congruences

$$A \equiv -\delta \cdot 10^{b_i} \pmod{p_i}, \quad 1 \leq i \leq t.$$

Then, for each $k \in \mathbb{Z}^+ \cup \{0\}$, the number

$$A + \delta \cdot 10^k$$

is divisible by at least one of the primes p_i where $1 \leq i \leq t$.

Proof. Suppose the conditions in the lemma hold. Let $k \in \mathbb{Z}^+ \cup \{0\}$. By (i), there is an $i \in \{1, \ldots, t\}$ such that $k \equiv b_i \pmod{c(p_i)}$. Write $k = c(p_i)q + b_i$. Since $c(p_i)$ is the multiplicative order of 10 modulo p_i, we have $10^{c(p_i)q} \equiv 1 \pmod{p_i}$. Hence,

$$A + \delta \cdot 10^k \equiv A + \delta \cdot 10^{b_i} \pmod{p_i}.$$

From (ii), we deduce $A + \delta \cdot 10^k \equiv 0 \pmod{p_i}$, completing the proof. □

We will determine an explicit example of primes $p_1, \ldots, p_t$ satisfying the conditions in Lemma 2.2 for each $\delta \in \{0, \ldots, 9\}$. We will denote this set of primes $\{p_1, \ldots, p_t\}$ by $\mathcal{P}_\delta$. The idea is to consider primes $p \equiv A \pmod{p_1 \cdots p_t}$ so that when a digit of p is increased by δ, the resulting number is divisible by some p_i with $1 \leq i \leq t$ (as the lemma implies). In order for primes p to exist with $p \equiv A \pmod{p_1 \cdots p_t}$, we will require $\gcd(A, p_1 \cdots p_t) = 1$.

We now proceed to choose for each $\delta \in \{1, \ldots, 9\}$ appropriate A, primes $p_1, \ldots, p_t$, and corresponding $b_1, \ldots, b_t$ so that (i) and (ii) of Lemma 2.2 hold. For $\delta \in \{2, 5, 8\}$, we take $A \equiv -2 \pmod{3}$ and

$$\mathcal{P}_2 = \mathcal{P}_5 = \mathcal{P}_8 = \{3\}.$$

In other words, for $\delta \in \{2, 5, 8\}$, we take $t = 1$ and $p_1 = 3$. As $c(3) = 1$, we can take $b_1 = 0$. Observe then that (i) and (ii) of Lemma 2.2 hold. Also, with $A \equiv -2 \pmod{3}$, we see that $\gcd(A, 3) = 1$. This application of Lemma 2.2 can be viewed as a degenerate case, where the covering of the integers in (i) is the single congruence $k \equiv 0 \pmod{1}$.

For our subsequent choices, we will make use of the factorizations of $10^n \pm 1$ in [3] to find primes p so that $n = c(p)$. For example, one checks that

$$\begin{aligned} 2 &= c(11), \quad & 4 &= c(101), \\ 8 &= c(73), \quad & 8 &= c(137). \end{aligned}$$

Thus, if we can find a covering of the integers which uses the moduli 2 and 4 each once and the modulus 8 twice, we can obtain congruences on A as in Lemma 2.2 (ii) to guarantee that for a fixed choice of δ, some prime in $\{11, 73, 101, 137\}$ divides each of the numbers $A + \delta \cdot 10^k$ for $k \in \mathbb{Z}^+ \cup \{0\}$. One checks that

$$\begin{aligned} k &\equiv 1 \pmod 2 \\ k &\equiv 2 \pmod 4 \\ k &\equiv 0 \pmod 8 \\ k &\equiv 4 \pmod 8 \end{aligned}$$

is such a covering of the integers. We take $\delta = 7$ and ensure Lemma 2.2 (ii) holds by taking

$$\begin{aligned} A &\equiv -7 \cdot 10^1 \equiv 7 \pmod{11}, \\ A &\equiv -7 \cdot 10^2 \equiv 7 \pmod{101}, \\ A &\equiv -7 \cdot 10^0 \equiv -7 \pmod{73}, \\ A &\equiv -7 \cdot 10^4 \equiv 7 \pmod{137}. \end{aligned}$$

Then since the conditions of Lemma 2.2 are satisfied, all of the numbers $A+7\cdot 10^k$ are divisible by some prime in the set $\mathcal{P}_7 = \{11, 73, 101, 137\}$. The Chinese Remainder Theorem implies that the four congruences above of the form $A \equiv -7 \cdot 10^k$ together with the congruence $A \equiv -2 \pmod 3$ are all equivalent to a single congruence modulo the product of the primes in $\mathcal{P}_2 \cup \mathcal{P}_5 \cup \mathcal{P}_7 \cup \mathcal{P}_8 = \{3, 11, 73, 101, 137\}$. Taking A to satisfy this single congruence, we have that for $\delta \in \{2, 5, 7, 8\}$ the numbers $A+\delta\cdot 10^k$, where $k \in \mathbb{Z}^+ \cup \{0\}$, are divisible by some prime in

$$\mathcal{P}_2 \cup \mathcal{P}_5 \cup \mathcal{P}_7 \cup \mathcal{P}_8 = \{3, 11, 73, 101, 137\}.$$

Furthermore, we have A is not divisible by primes in $\{3, 11, 73, 101, 137\}$ so that there are primes $p \equiv A \pmod{3 \cdot 11 \cdot 73 \cdot 101 \cdot 137}$.

We continue in this way, finding for each $\delta \in \{1, 3, 4, 6, 9\}$ coverings

$$k \equiv b_i \pmod{c(p_i)}$$

with corresponding congruences $A \equiv -\delta \cdot 10^{b_i} \pmod{p_i}$. To allow these congruences to occur simultaneously with congruences already established, our choices will either utilize p_i distinct from those used before or will be equivalent to congruences already established. For example, we have $A \equiv 7 \pmod{11}$ above, so it follows that

$$A \equiv -4 \cdot 10^0 \pmod{11}.$$

Recall $c(11) = 2$. Thus, taking $k \equiv 0 \pmod{2}$ in (i) of Lemma 2.2 and taking $\delta = 4$, we see that (ii) of Lemma 2.2 holds for the prime 11. In other words, we may re-use $c(11) = 2$ as a modulus in a covering corresponding to $\delta = 4$ so long as we choose $k \equiv 0 \pmod{2}$. Table 2.1 exhibits such a covering, where in the table we have made use of the notation

$$p_{10} = 9999999900000001, \quad p_{19} = 15343168188889137818369,$$

$$p_{20} = 5152175252652132674478699068158 73, \quad p_{24} = 1253224535459902849,$$

$$p_{25} = 53763491189967221358575546107279034709697.$$

To clarify, we are taking $\mathcal{P}_4$ to be the set of 27 primes appearing in Table 2.1 in the columns with heading "prime p_i". One checks that the columns with heading "congruence" in Table 2.1 describe a covering of the integers. Note that the least common multiple of the moduli appearing in this system of congruences is 768, so checking that a covering of the integers is indeed described in Table 2.1 amounts to verifying that each of the numbers $0, 1, \ldots, 767$ satisfies some congruence in Table 2.1. One further checks that each prime number p_i in the columns with heading "prime p_i" indeed has $c(p_i)$ equal to the modulus appearing in that row. This suffices to show that the congruences in Table 2.1 satisfy (i) in Lemma 2.2. Thus, with $\delta = 4$

Table 2.1 Covering used in Lemma 2.2 (i) for $A + 4 \cdot 10^k$

row	congruence	prime p_i
1	$k \equiv 0 \pmod 2$	11
2	$k \equiv 1 \pmod 6$	7
3	$k \equiv 1 \pmod{16}$	17
4	$k \equiv 9 \pmod{16}$	5882353
5	$k \equiv 3 \pmod{32}$	353
6	$k \equiv 11 \pmod{32}$	449
7	$k \equiv 19 \pmod{32}$	641
8	$k \equiv 27 \pmod{32}$	1409
9	$k \equiv 5 \pmod{32}$	69857
10	$k \equiv 23 \pmod{48}$	p_{10}
11	$k \equiv 13 \pmod{64}$	19841
12	$k \equiv 21 \pmod{64}$	976193
13	$k \equiv 29 \pmod{64}$	6187457
14	$k \equiv 45 \pmod{64}$	834427406578561
15	$k \equiv 15 \pmod{96}$	97
16	$k \equiv 39 \pmod{96}$	206209
17	$k \equiv 63 \pmod{96}$	66554101249
18	$k \equiv 87 \pmod{96}$	75118313082913
19	$k \equiv 53 \pmod{128}$	p_{19}
20	$k \equiv 117 \pmod{128}$	p_{20}
21	$k \equiv 61 \pmod{128}$	1265011073
22	$k \equiv 47 \pmod{192}$	193
23	$k \equiv 95 \pmod{192}$	769
24	$k \equiv 143 \pmod{192}$	p_{24}
25	$k \equiv 191 \pmod{192}$	p_{25}
26	$k \equiv 125 \pmod{256}$	257
27	$k \equiv 253 \pmod{256}$	15361

and taking A to be a solution to the corresponding congruences in Lemma 2.2 (ii), e.g., from row 9 we take

$$A \equiv -4 \cdot 10^5 \pmod{69857},$$

we have from Lemma 2.2 that for all $k \in \mathbb{Z}^+ \cup \{0\}$, the number $A + 4 \cdot 10^k$ is divisible by some prime in $\mathcal{P}_4$. Thus, for any number A satisfying the system of congruences already established, we have for $\delta \in \{2, 4, 5, 7, 8\}$ that the numbers $A + \delta \cdot 10^k$ are divisible by some prime $p \in \mathcal{P}_2 \cup \mathcal{P}_4 \cup \mathcal{P}_5 \cup \mathcal{P}_7 \cup \mathcal{P}_8$.

For $\delta \in \{1, 6, 9\}$, we utilize the remaining coverings appearing in [10], which we reproduce here in Tables 2.2, 2.3, and 2.4. The following notation for primes are used in these tables:

$$p_7 = 440334654777631, \quad p_9 = 5964848081, \quad p_{11} = 1025988002321111471,$$

$$p_{12} = 3199044596370769, \quad p_{13} = 265212793249617641,$$

$$p_{14} = 30703738801, \quad p_{15} = 625437743071,$$

$$p_{16} = 57802050308786191965409441, \quad p_{17} = 4185502830133110721,$$

$$p_{21} = 4458192223320340849, \quad p_{27} = 127522001020150503761,$$

$$p_{31} = 60368344121, \quad p_{32} = 848654483879497562821,$$

$$p_{34} = 73765755896403138401, \quad p_{35} = 11189053009,$$

$$p_{36} = 603812429055411913, \quad p_{37} = 148029423400750506553.$$

Table 2.2 Covering used in Lemma 2.2 (i) for $A + 1 \cdot 10^k$

row	congruence	prime p_i
1	$k \equiv 0 \pmod 3$	37
2	$k \equiv 1 \pmod 6$	13
3	$k \equiv 2 \pmod 9$	333667
4	$k \equiv 5 \pmod{18}$	19
5	$k \equiv 14 \pmod{18}$	52579
6	$k \equiv 8 \pmod{27}$	757
7	$k \equiv 17 \pmod{27}$	p_7

row	congruence	prime p_i
8	$k \equiv 26 \pmod{54}$	70541929
9	$k \equiv 53 \pmod{54}$	14175966169
10	$k \equiv 4 \pmod{12}$	9901
11	$k \equiv 10 \pmod{24}$	99990001
12	$k \equiv 22 \pmod{72}$	p_{12}
13	$k \equiv 46 \pmod{72}$	3169
14	$k \equiv 70 \pmod{72}$	98641

Table 2.3 Covering used in Lemma 2.2 (i) for $A + 6 \cdot 10^k$

row	congruence	prime p_i
1	$k \equiv 0 \pmod 5$	41
2	$k \equiv 1 \pmod 5$	271
3	$k \equiv 2 \pmod{10}$	9091
4	$k \equiv 3 \pmod{20}$	3541
5	$k \equiv 13 \pmod{20}$	27961
6	$k \equiv 7 \pmod{30}$	211
7	$k \equiv 17 \pmod{30}$	241
8	$k \equiv 27 \pmod{30}$	2161
9	$k \equiv 8 \pmod{40}$	p_9
10	$k \equiv 28 \pmod{40}$	1676321

row	congruence	prime p_i
11	$k \equiv 18 \pmod{60}$	61
12	$k \equiv 38 \pmod{60}$	4188901
13	$k \equiv 58 \pmod{60}$	39526741
14	$k \equiv 4 \pmod{15}$	31
15	$k \equiv 9 \pmod{15}$	2906161
16	$k \equiv 14 \pmod{45}$	238681
17	$k \equiv 29 \pmod{45}$	p_{17}
18	$k \equiv 44 \pmod{90}$	29611
19	$k \equiv 89 \pmod{90}$	3762091

Taking A to simultaneously satisfy all the congruences corresponding to (ii) in Lemma 2.2, we have that for all $\delta \in \{1, 2, 4, 5, 6, 7, 8, 9\}$, each of the numbers $A+\delta \cdot 10^k$ is divisible by some prime $p \in \mathcal{P}_1 \cup \mathcal{P}_2 \cup \mathcal{P}_4 \cup \mathcal{P}_5 \cup \mathcal{P}_6 \cup \mathcal{P}_7 \cup \mathcal{P}_8 \cup \mathcal{P}_9$. We require one more covering system for $\delta = 3$.

For $\delta = 3$, we will make use of three primes previously used for other choices of δ, namely the prime 73 for $\delta = 7$ and the primes 7 and 17 for $\delta = 4$. From

Table 2.4 Covering used in Lemma 2.2 (i) for $A + 9 \cdot 10^k$

row	congruence	prime p_i
1	$k \equiv 0 \pmod 7$	239
2	$k \equiv 1 \pmod 7$	4649
3	$k \equiv 2 \pmod{21}$	43
4	$k \equiv 9 \pmod{21}$	1933
5	$k \equiv 16 \pmod{21}$	10838689
6	$k \equiv 3 \pmod{14}$	909091
7	$k \equiv 10 \pmod{28}$	29
8	$k \equiv 24 \pmod{28}$	281
9	$k \equiv 4 \pmod{35}$	71
10	$k \equiv 11 \pmod{35}$	123551
11	$k \equiv 18 \pmod{35}$	p_{11}
12	$k \equiv 25 \pmod{70}$	4147571
13	$k \equiv 60 \pmod{70}$	p_{13}
14	$k \equiv 32 \pmod{105}$	p_{14}
15	$k \equiv 67 \pmod{105}$	p_{15}
16	$k \equiv 102 \pmod{105}$	p_{16}
17	$k \equiv 5 \pmod{42}$	127
18	$k \equiv 26 \pmod{42}$	2689
19	$k \equiv 12 \pmod{42}$	459691

row	congruence	prime p_i
20	$k \equiv 33 \pmod{84}$	226549
21	$k \equiv 75 \pmod{84}$	p_{21}
22	$k \equiv 19 \pmod{63}$	10837
23	$k \equiv 40 \pmod{63}$	23311
24	$k \equiv 61 \pmod{63}$	45613
25	$k \equiv 6 \pmod{28}$	121499449
26	$k \equiv 13 \pmod{56}$	7841
27	$k \equiv 41 \pmod{56}$	p_{27}
28	$k \equiv 20 \pmod{140}$	421
29	$k \equiv 48 \pmod{140}$	3471301
30	$k \equiv 76 \pmod{140}$	13489841
31	$k \equiv 104 \pmod{140}$	p_{31}
32	$k \equiv 132 \pmod{140}$	p_{32}
33	$k \equiv 27 \pmod{112}$	113
34	$k \equiv 83 \pmod{112}$	p_{34}
35	$k \equiv 55 \pmod{168}$	p_{35}
36	$k \equiv 111 \pmod{168}$	p_{36}
37	$k \equiv 167 \pmod{168}$	p_{37}

our prior congruences, we have $A \equiv -7 \pmod{73}$, $A \equiv -4 \cdot 10 \equiv 2 \pmod 7$, and $A \equiv -4 \cdot 10 \equiv -6 \pmod{17}$. We make use of the equivalent congruences

$$\begin{aligned} A &\equiv -3 \cdot 10^3 \pmod{73}, \\ A &\equiv -3 \cdot 10^4 \pmod 7, \\ A &\equiv -3 \cdot 10^{10} \pmod{17} \end{aligned}$$

to help construct a covering for the case $\delta = 3$. Our choices for this covering will require primes where 10 has multiplicative order larger than that appearing in the tables in [3]. To find such primes, we obtain partial factorizations of $\Phi_n(10)$, where $\Phi_n(x)$ is the nth cyclotomic polynomial. We make use of the following facts regarding primes dividing $\Phi_n(10)$, which are discussed in [3, p. III C 1]. Let p be a prime dividing $\Phi_n(10)$.

- If $p > n$, we have $c(p) = n$ and $p \equiv 1 \pmod n$.

- If $p \leq n$ and $n > 2$, then p is the largest prime dividing n and $\nu_p(\Phi_n(10)) = 1$.

To find a lower bound on the number of primes p having $c(p) = n$, we first determine whether the largest prime q dividing n also divides $\Phi_n(10)$. We then look for distinct small primes $p_1, \ldots, p_r$ with $p_j \equiv 1 \pmod{n}$ and $p_j | \Phi_n(10)$. Note that the condition $p_j \equiv 1 \pmod{n}$ helps narrow the search space of primes to consider. Once this calculation is complete, we verify that $\gcd\left(\Phi_n(10)/\prod_{i=1}^r p_i, \prod_{i=1}^r p_i\right) = 1$. We then use the `is_prime_power()` routine in Sage to verify that $\Phi_n(10)/\prod_{i=1}^r p_i$ (or alternatively $\Phi_n(10)/(q\prod_{i=1}^r p_i)$ if $q \mid \Phi_n(10)$) is neither 1 nor a prime power. If this quotient is 1, we have at least r distinct primes p with $c(p) = n$. If the quotient is a prime power, we have at least $r+1$ distinct primes p with $c(p) = n$. If the quotient is not a prime power and not 1, we have at least $r+2$ distinct primes p with $c(p) = n$. In the latter case, although the additional two primes can be determined with enough computation, we do not need them explicitly for the proof of Theorem 1.3.

Table 2.5 displays the results of these computations of prime divisors of $\Phi_n(10)$. Each n we consider has largest prime divisor $q = 11$ and only $n = 242$ has $11 \mid \Phi_n(10)$. In Table 2.5, we write $\Phi_n(10) = p_1 p_2 \cdots p_r C_n$, where C_n is a composite factor of $\Phi_n(10)$ having at least 2 distinct prime divisors different from $p_1, p_2, \ldots, p_r$. We write $\Phi_n(10) = p_1 p_2 \cdots p_r P_n$, where P_n is a prime factor of $\Phi_n(10)$ different from $p_1, p_2, \ldots, p_r$. Computationally, P_n was determined to be a prime power and then verified to be a prime. In the tables that follow, we denote by $p_{n,1}$ and $p_{n,2}$ the two smallest prime divisors of C_n. We did not compute the values of $p_{n,1}$ and $p_{n,2}$, but we know they exist. We also included some values of n in Table 2.5 which appear in [3] since this notation allows us to avoid displaying lengthy primes.

Table 2.6, Table 2.7, and Table 2.8 display the covering system of the integers corresponding to the case $\delta = 3$ in Lemma 2.2 (i). To conserve space, we set

$$p_{18} = 162058348460129675849270826564021069 53,$$

Table 2.5 Partial factorizations of $\Phi_n(10)$ for large n

n	Partial factorization of $\Phi_n(10)$
121	$15973 \cdot 38237 \cdot 274187 \cdot P_{121}$
242	$11 \cdot 4357 \cdot 25169 \cdot 1485397 \cdot C_{242}$
275	$7151 \cdot 15401 \cdot 59951 \cdot C_{275}$
363	$622001227 \cdot C_{363}$
396	$79082656489 \cdot C_{396}$
484	$56629 \cdot 170369 \cdot 29606281 \cdot 149116408676012825500 1869 \cdot C_{484}$
605	C_{605}
726	$727 \cdot 1453 \cdot C_{726}$
792	$761113 \cdot C_{792}$
1188	$765144469 \cdot C_{1188}$
1210	$10891 \cdot 131891 \cdot C_{1210}$
1452	P_{1452}
2420	$1006721 \cdot 2323201 \cdot 1754328181 \cdot C_{2420}$
2904	C_{2904}
4356	$949609 \cdot 384538969 \cdot C_{4356}$
5808	$21582529 \cdot 114690577 \cdot C_{5808}$

$$p_{42} = 13826777012791645762903 4873443951,$$

$$p_{43} = 17035489138924940750976645620238442780 44121,$$

$$p_{44} = 13959003709163272455554419 01,$$

$$p_{45} = 36380545029953205956377406702261,$$

$$p_{48} = 11123141013112860033797526178078704096112852 81,$$

$$p_{52} = 13661466857600232937149644755591574091018104 3,$$

$$p_{62} = 36285372434299046932476623547426886978631188605 3883,$$

$$p_{64} = 14112252487788618228223353931779614493830511116 8717,$$

$$p_{75} = 79070093075946940010535520005886583911009740934576037164194 37,$$

$$p_{77} = 89272446239411813982332 53, \quad p_{78} = 18667635465676809961034173760 59,$$

$$p_{79} = 11297030838243985940172694734174070455495173740851135 4573,$$

$$p_{80} = 74507557122096964531006066514788984423438931950911932421947947339.$$

Table 2.6 First part of covering used for $A + 3 \cdot 10^k$

row	congruence	prime p_i
1	$k \equiv 4 \pmod 6$	7
2	$k \equiv 3 \pmod 8$	73
3	$k \equiv 0 \pmod{11}$	21649
4	$k \equiv 1 \pmod{11}$	513239
5	$k \equiv 10 \pmod{16}$	17
6	$k \equiv 2 \pmod{22}$	23
7	$k \equiv 13 \pmod{22}$	4093
8	$k \equiv 3 \pmod{22}$	8779
9	$k \equiv 14 \pmod{44}$	89
10	$k \equiv 36 \pmod{44}$	1052788969
11	$k \equiv 15 \pmod{33}$	67
12	$k \equiv 26 \pmod{33}$	13446282103132983 73
13	$k \equiv 37 \pmod{66}$	599144041
14	$k \equiv 38 \pmod{132}$	5419170769
15	$k \equiv 126 \pmod{132}$	789390798020221
16	$k \equiv 60 \pmod{132}$	2361000305507449
17	$k \equiv 5 \pmod{88}$	617
18	$k \equiv 49 \pmod{88}$	p_{18}
19	$k \equiv 104 \pmod{264}$	2377
20	$k \equiv 236 \pmod{264}$	16369
21	$k \equiv 71 \pmod{264}$	432961

row	congruence	prime p_i
22	$k \equiv 159 \pmod{264}$	6796152793
23	$k \equiv 247 \pmod{264}$	24387741577
24	$k \equiv 6 \pmod{55}$	1321
25	$k \equiv 17 \pmod{55}$	62921
26	$k \equiv 28 \pmod{55}$	83251631
27	$k \equiv 39 \pmod{55}$	1300635692678058358830121
28	$k \equiv 50 \pmod{110}$	331
29	$k \equiv 105 \pmod{110}$	5171
30	$k \equiv 7 \pmod{110}$	20163494891
31	$k \equiv 62 \pmod{110}$	318727841165674579776721
32	$k \equiv 18 \pmod{220}$	661
33	$k \equiv 73 \pmod{220}$	18041
34	$k \equiv 128 \pmod{220}$	148721
35	$k \equiv 183 \pmod{220}$	1121407321
36	$k \equiv 40 \pmod{275}$	7151
37	$k \equiv 95 \pmod{275}$	15401
38	$k \equiv 150 \pmod{275}$	59951
39	$k \equiv 205 \pmod{275}$	$p_{275,1}$
40	$k \equiv 260 \pmod{275}$	$p_{275,2}$
41	$k \equiv 29 \pmod{165}$	471241
42	$k \equiv 84 \pmod{165}$	p_{42}

Table 2.7 Second part of covering used for $A + 3 \cdot 10^k$

row	congruence	prime p_i
43	$k \equiv 139 \pmod{165}$	p_{43}
44	$k \equiv 51 \pmod{220}$	p_{44}
45	$k \equiv 161 \pmod{220}$	p_{45}
46	$k \equiv 106 \pmod{330}$	4124507971
47	$k \equiv 216 \pmod{330}$	19835636682880495867311241
48	$k \equiv 326 \pmod{330}$	p_{48}
49	$k \equiv 8 \pmod{77}$	5237
50	$k \equiv 19 \pmod{77}$	42043
51	$k \equiv 30 \pmod{77}$	29920507
52	$k \equiv 41 \pmod{77}$	p_{52}
53	$k \equiv 52 \pmod{154}$	463
54	$k \equiv 129 \pmod{154}$	24179
55	$k \equiv 63 \pmod{154}$	590437
56	$k \equiv 140 \pmod{154}$	7444361
57	$k \equiv 74 \pmod{154}$	4539402627853030477
58	$k \equiv 151 \pmod{154}$	4924630160315726207887
59	$k \equiv 9 \pmod{99}$	199
60	$k \equiv 20 \pmod{99}$	397
61	$k \equiv 31 \pmod{99}$	34849
62	$k \equiv 42 \pmod{99}$	p_{62}
63	$k \equiv 53 \pmod{198}$	7093127053

row	congruence	prime p_i
64	$k \equiv 152 \pmod{198}$	p_{64}
65	$k \equiv 64 \pmod{396}$	79082656489
66	$k \equiv 163 \pmod{396}$	$p_{396,1}$
67	$k \equiv 262 \pmod{396}$	$p_{396,2}$
68	$k \equiv 361 \pmod{792}$	761113
69	$k \equiv 757 \pmod{792}$	$p_{792,1}$
70	$k \equiv 75 \pmod{297}$	55243
71	$k \equiv 174 \pmod{297}$	198397
72	$k \equiv 273 \pmod{297}$	1981560241
73	$k \equiv 86 \pmod{297}$	31600574312077
74	$k \equiv 185 \pmod{297}$	165426670443186506567467
75	$k \equiv 284 \pmod{297}$	p_{75}
76	$k \equiv 97 \pmod{594}$	7129
77	$k \equiv 196 \pmod{594}$	p_{77}
78	$k \equiv 295 \pmod{594}$	p_{78}
79	$k \equiv 394 \pmod{594}$	p_{79}
80	$k \equiv 493 \pmod{594}$	p_{80}
81	$k \equiv 592 \pmod{1188}$	765144469
82	$k \equiv 1186 \pmod{1188}$	$p_{1188,1}$
83	$k \equiv 10 \pmod{121}$	15973
84	$k \equiv 21 \pmod{121}$	38237

Table 2.8 Third part of covering used for $A + 3 \cdot 10^k$

row	congruence	prime p_i
85	$k \equiv 32 \pmod{121}$	274187
86	$k \equiv 43 \pmod{121}$	P_{121}
87	$k \equiv 54 \pmod{242}$	4357
88	$k \equiv 175 \pmod{242}$	25169
89	$k \equiv 65 \pmod{242}$	1485397
90	$k \equiv 186 \pmod{242}$	$p_{242,1}$
91	$k \equiv 76 \pmod{242}$	$p_{242,2}$
92	$k \equiv 197 \pmod{484}$	56629
93	$k \equiv 439 \pmod{484}$	170369
94	$k \equiv 87 \pmod{484}$	29606281
95	$k \equiv 208 \pmod{484}$	14911640867601282550018 69
96	$k \equiv 329 \pmod{484}$	$p_{484,1}$
97	$k \equiv 450 \pmod{484}$	$p_{484,2}$
98	$k \equiv 98 \pmod{363}$	622001227
99	$k \equiv 219 \pmod{363}$	$p_{363,1}$
100	$k \equiv 340 \pmod{363}$	$p_{363,2}$
101	$k \equiv 109 \pmod{726}$	727
102	$k \equiv 230 \pmod{726}$	1453
103	$k \equiv 351 \pmod{726}$	$p_{726,1}$
104	$k \equiv 472 \pmod{726}$	$p_{726,2}$

row	congruence	prime p_i
105	$k \equiv 593 \pmod{1452}$	P_{1452}
106	$k \equiv 1319 \pmod{4356}$	949609
107	$k \equiv 2771 \pmod{4356}$	384538969
108	$k \equiv 4223 \pmod{4356}$	$p_{4356,1}$
109	$k \equiv 714 \pmod{2904}$	$p_{2904,1}$
110	$k \equiv 1440 \pmod{2904}$	$p_{2904,2}$
111	$k \equiv 2166 \pmod{5808}$	21582529
112	$k \equiv 5070 \pmod{5808}$	114690577
113	$k \equiv 2892 \pmod{5808}$	$p_{5808,1}$
114	$k \equiv 5796 \pmod{5808}$	$p_{5808,2}$
115	$k \equiv 120 \pmod{605}$	$p_{605,1}$
116	$k \equiv 241 \pmod{605}$	$p_{605,2}$
117	$k \equiv 362 \pmod{1210}$	10891
118	$k \equiv 967 \pmod{1210}$	131891
119	$k \equiv 483 \pmod{1210}$	$p_{1210,1}$
120	$k \equiv 1088 \pmod{1210}$	$p_{1210,2}$
121	$k \equiv 604 \pmod{2420}$	1006721
122	$k \equiv 1209 \pmod{2420}$	2323201
123	$k \equiv 1814 \pmod{2420}$	1754328181
124	$k \equiv 2419 \pmod{2420}$	$p_{2420,1}$

Taking A to satisfy the corresponding congruences in Lemma 2.2 (ii) with $\delta = 3$, we have that $A + 3 \cdot 10^k$ is divisible by some prime p_i appearing in the columns with heading "prime p_i" in Tables 2.6, 2.7, and 2.8. For the remainder of the paper, we will set

$$M = \prod_{\delta \in \{1,2,\ldots,8,9\}} \prod_{p \in \mathcal{P}_\delta} p$$

and will take A to be the unique residue class modulo M satisfying all the congruences in Lemma 2.2 (ii) we have constructed for $\delta \in \{1, 2, \ldots, 8, 9\}$. Note that each of the congruences $A \equiv -\delta \cdot 10^{b_i} \pmod{p_i}$ describe nonzero residue classes modulo p_i. For $p_i = 3$ and $p_i = 7$, we avoided $\delta \equiv 0 \pmod{p_i}$ and for all other p_i appearing above, $p_i > 10$ ensures that $-\delta \cdot 10^{b_i}$ is nonzero. Thus, we have $\gcd(A, M) = 1$. Based on our work so far, if p is a prime with $p \equiv A \pmod{M}$, then $p + \delta \cdot 10^k$ is divisible by a prime dividing M for every choice of $\delta \in \{1, 2, \ldots, 9\}$ and $k \in \mathbb{Z}^+ \cup \{0\}$. We now proceed to $\delta \in \{-9, -8, \ldots, -2, -1\}$.

2.2 Decreasing a digit

Let K be a large integer. Our goal is to estimate the number of digitally delicate primes p with $p \equiv A \pmod{M}$ and with p having $\leq K$ digits. Observe that the number of digit changes for such p is at most $9K$. As noted above, we have that $p + \delta \cdot 10^j$, for $0 \leq j < K$ and $\delta \in \{1, 2, \ldots, 8, 9\}$, is divisible by a prime dividing M. For $p > M$ and for $0 \leq j < K$ and $\delta \in \{1, 2, \ldots, 8, 9\}$, we deduce then that $p + \delta \cdot 10^j$ is composite. We extend this to the $9K$ more numbers $p + \delta \cdot 10^j$ where $0 \leq j < K$ and $\delta \in \{-9, -8, \ldots, -2, -1\}$.

We begin with an idea of P. Erdős to dispense with most of these $9K$ possibilities by considering primes p only in residue classes modulo some primes for which 10 has small order. To be more precise, suppose k_0 is the smallest value of the order of 10 modulo a prime divisor of M. Fix $\varepsilon > 0$, and let $K_0 = K_0(\varepsilon)$ be a positive integer to be specified momentarily. Note that with k_0 fixed as above, the value of K_0 will

depend only on ε, and K will be taken to be large in comparison to K_0. For each integer $c \in (k_0, K_0]$, we know there exists a prime q_c such that 10 has order c modulo q_c (cf. [1], [31]). A result of Stewart [29] implies that we can take

$$q_c > k_1 c \cdot (\log c)^2, \tag{2.1}$$

for some constant $k_1 > 0$ (depending on k_0). We proceed with the q_c so chosen. Since the order of 10 modulo primes dividing M are $\leq k_0$, no q_c divides M.

We will restrict our attention to primes $c \in (k_0, K_0]$. We want to use most of these primes and separate them into 9 sets depending on $\delta \in \{-9, -8, \ldots, -2, -1\}$. For this purpose, we define

$$\mathcal{Q}_\delta = \{c \in (k_0, K_0] : c \text{ prime}, c \equiv \delta \pmod{11}\}.$$

We set

$$\mathcal{Q} = \bigcup_{\delta \in \{-9,-8,\ldots,-1\}} \mathcal{Q}_\delta, \qquad M' = \prod_{\delta \in \{-9,-8,\ldots,-1\}} \prod_{c \in \mathcal{Q}_\delta} q_c, \qquad \text{and} \qquad W = MM'.$$

For each $\delta \in \{-9, -8, \ldots, -2, -1\}$, we consider

$$p \equiv -\delta \pmod{\prod_{c \in \mathcal{Q}_\delta} q_c}.$$

By the Chinese Remainder Theorem, there is a $B \in \mathbb{Z}$ such that these 9 congruences, one for each $\delta \in \{-9, -8, \ldots, -2, -1\}$, are equivalent to a single congruence $p \equiv B \pmod{M'}$. As a consequence, we have that if $p \equiv B \pmod{M'}$ and $\delta \in \{-9, -8, \ldots, -2, -1\}$, then for every nonnegative integer k that is divisible by a $c \in \mathcal{Q}_\delta$, we have $p + \delta \cdot 10^k$ is divisible by the prime q_c. Thus, with fixed $p \equiv B \pmod{M'}$ and fixed $\delta \in \{-9, -8, \ldots, -2, -1\}$, an inclusion-exclusion argument shows that the number of integers $j \in (0, K]$ with $p + \delta \cdot 10^j$ relatively prime to M' is

$$\leq K \prod_{c \in \mathcal{Q}_\delta} \left(1 - \frac{1}{c}\right) + O\big(2^{K_0}\big). \tag{2.2}$$

We take $K_0 = K_0(\varepsilon)$ so that for K sufficiently large, the expression in (2.2) is $< \varepsilon K$, which is possible since $\sum^*_{c>k_0} 1/c$ diverges where the $*$ indicates the sum is over primes $c \equiv \delta \pmod{11}$.

Since $\gcd(M, M') = 1$, the primes p which are A modulo M and B modulo M' correspond to the primes in a single congruence class, say w, modulo $W = MM'$. We now have that if $p \equiv w \pmod{W}$, then for all but $< 9\varepsilon K$ choices of $0 \leq j < K$ and $\delta \in \{-9, -8, \ldots, -2, -1\} \cup \{1, 2, \ldots, 8, 9\}$, the number $p + \delta \cdot 10^j$ is divisible by a prime dividing W. Furthermore, the choices for $\delta \cdot 10^j$ for which $p + \delta \cdot 10^j$ is divisible by a prime dividing W depend only on the residue class w modulo W and, hence, do not depend on the prime $p \equiv w \pmod{W}$. Let H denote the set of $\delta \cdot 10^j$ with $0 \leq j < K$ and $\delta \in \{-9, -8, \ldots, -2, -1\} \cup \{1, 2, \ldots, 8, 9\}$ such that the number $p + \delta \cdot 10^j$ is not divisible by a prime dividing W for $p \equiv w \pmod{W}$. For our purposes, we can in fact take H to be the numbers of the form $\delta \cdot 10^j$, where $\delta \in \{-9, -8, \ldots, -2, -1\}$ and j is not divisible by any $c \in \mathcal{Q}_\delta$. Note that $|H|$, the size of H, is bounded above by $9\varepsilon K$.

We continue with an idea of Tao [30] and recall a theorem from sieve theory (cf. [13, Theorem 2.4], [30]).

Theorem 2.3. *Let W and w be positive integers, and let h be a non-zero integer. If x is sufficiently large (depending on W and w), then the number of primes $p \leq x$ with $p \equiv w \pmod{W}$ and $p + h$ prime is*

$$\leq \frac{C\,x}{\phi(W)(\log x)^2} \prod_{\substack{q \text{ prime} \\ q \mid (hW)}} \left(1 - \frac{1}{q}\right)^{-1},$$

where C is an absolute constant.

Of some significance here is that C does not depend on h. For our purposes, we want $h = \delta \cdot 10^j \in H$. Thus, the primes dividing h belong to the finite set $\{2, 3, 5, 7\}$. We also view M and M' and, hence, W as fixed. We take $x = 10^K$ with K large depending on ε. For each of the $h = \delta \cdot 10^j \in H$, we apply Theorem 2.3.

Recall that the primes dividing W appearing in the product in Theorem 2.3 include the primes q_c for $c \in \mathcal{Q}$ and $\mathcal{Q}$ depends on K_0 and K_0 depends on ε. We will use a lower bound on this product appearing in the theorem to get rid of its dependence on ε. More precisely, recalling (2.1) and that the primes dividing h belong to the set $\{2, 3, 5, 7\}$, we see that

$$\prod_{\substack{q \text{ prime} \\ q|(hW)}} \left(1 - \frac{1}{q}\right) \geq \frac{8}{35} \prod_{\substack{q \text{ prime} \\ q|W}} \left(1 - \frac{1}{q}\right) > \frac{8}{35} \prod_{\substack{p \text{ prime} \\ p|M}} \left(1 - \frac{1}{p}\right) \prod_{\substack{c \text{ prime} \\ k_0 < c \leq K_0}} \left(1 - \frac{1}{q_c}\right)$$
$$> \frac{8}{35} \prod_{\substack{p \text{ prime} \\ p|M}} \left(1 - \frac{1}{p}\right) \prod_{k_0 < c \leq K_0} \left(1 - \frac{1}{k_1 c (\log c)^2}\right).$$

As the sum $\sum_{c > k_0} 1/(c(\log c)^2)$ converges, we see that, for a fixed $h \in H$, there is a constant $C' = C'(M)$, independent of $\varepsilon > 0$, such that there are at most $C'x/(\phi(W)\log^2 x)$ primes $p \leq x$ with $p \equiv w \pmod{W}$ and $p + h$ prime. Letting h vary over the elements of H, the total number of primes $p \leq x$ with $p \equiv w \pmod{W}$ and $p + h$ prime for some $h \in H$ is bounded above by

$$\frac{|H| \cdot C'x}{\phi(W)\log^2 x} < \frac{9\varepsilon K C'x}{\phi(W)\log^2 x} = \frac{9\varepsilon C'x}{\phi(W)\log(10) \cdot \log x}.$$

The remaining primes $p \leq x$ with $p \equiv w \pmod{W}$ satisfy that $p + h$ is composite for every $h \in H$. Thus, these remaining primes will be digitally delicate. By the Prime Number Theorem for Arithmetic Progressions, the total number of primes $p \leq x = 10^K$ with $p \equiv w \pmod{W}$ and K large is $> x/(2\phi(W)\log x)$. By taking ε sufficiently small and, hence, K sufficiently large, we see that there are a positive proportion of primes $p \leq x = 10^K$ with $p \equiv w \pmod{W}$ that are digitally delicate. As these primes satisfy $p \equiv A \pmod{M}$, we deduce that a positive proportion of primes up to 10^K are widely digitally delicate. As a positive proportion of primes up to 10^K is still a positive proportion of primes up to 10^{K+1}, we can see that the restriction of x to the form 10^K can be eliminated and there is a uniform lower bound on the proportion of primes up to x, for x large, that are widely digitally delicate. This establishes Theorem 1.3.

2.3 Related topics and open problems

Questions related to Theorem 1.3 abound. Carl Pomerance (private communication) has asked about primes which are not digitally or widely digitally delicate. In this regard the simplest question one could ask is whether there are infinitely many primes which are not digitally delicate. The prime k-tuple conjecture states that every admissible pattern for a prime constellation occurs infinitely often. If one assumes this conjecture, then in the case $k = 3$ we obtain there are an infinite number of primes p for which $p - 2$ and $p + 4$ are also prime. Then for any base $b > 6$ express such p in base b as

$$p = d_k \cdots d_1 d_0 = d_k b^k + \cdots + d_1 b + d_0$$

where $0 \leq d_i \leq b - 1$. Then if $d_0 > 2$, we have that $p - 2$ corresponds to changing a digit of p in base b. If alternatively $d_0 < b - 4$, we obtain that $p + 4$ corresponds to changing a digit of p in base b. Since for $b > 6$ we must have either $d_0 > 2$ or $d_0 < b - 4$, the prime p in such a constellation cannot be digitally delicate in base b. Thus an infinite number of primes are not digitally delicate.

Apart from utilizing a conjecture, we have been unable to establish an unconditional proof of the infinitude of primes which are not digitally delicate. What is surprising in this regard is that computationally it appears as if the proportion of digitally delicate primes is *less* than the proportion of non-digitally delicate primes. For each of the bases $b \in \{2, 3, \cdots, 10\}$ and each of the intervals $(10^{100}, 10^{125})$, $(10^{125}, 10^{150})$, $(10^{150}, 10^{175})$, $(10^{175}, 10^{200})$, we generated 100000 primes in the given interval and counted the number of primes out of the 100000 that were digitally delicate in that base. We use the notation $\mathcal{L}_b(k, \ell)$ in Table 2.9 to represent the number of primes out of 100000 in the interval $(10^k, 10^\ell)$ that were digitally delicate in base b.

The proportions seem to be constant for a fixed base, with the largest proportion appearing when $b = 3$ at around 21% of primes being digitally delicate in base 3.

Table 2.9 $\mathcal{L}_b(k, \ell)$ for bases $b \in \{2, 3, \cdots, 10\}$

b	2	3	4	5	6	7	8	9	10
$\mathcal{L}_b(100, 125)$	16246	20860	4159	18166	75	9976	375	1520	18
$\mathcal{L}_b(125, 150)$	16319	20641	4285	18171	68	10270	406	1513	12
$\mathcal{L}_b(150, 175)$	16352	20736	4383	18396	66	10063	417	1510	15
$\mathcal{L}_b(175, 200)$	16385	20747	4280	18212	65	10223	376	1474	12

However, perhaps this pattern changes as the primes involved grow. Such a determination could be made with more computational effort.

One discernible pattern in Table 2.9 that bears out theoretically is the diminishing proportion of primes that are digitally delicate in bases which are non-prime powers of primes. One can see in Table 2.9 that the proportions for 4, 8, and 9 are much smaller than the proportions for any of the primes 2, 3, 5, 7. This is because a change of a single digit of p in base b implies a change of a single digit of p in base b^t, so that the following holds.

Lemma 2.4. *Let b be an integer greater than 1 and let p be a prime digitally delicate in base b^t, $t \geq 1$. Then p is digitally delicate in base b as well.*

This result does not hold for arbitrary composite bases. For example, the prime 28151 is digitally delicate in base 6 but not in base 2 or base 3. Despite this non-implication, it appears from the columns $b = 6$, $b = 10$ in Table 2.9 that the proportion of digitally delicate primes decreases as the number of divisors of b increases.

Moving beyond the basic question of their infinitude, one could also ask whether a positive proportion of primes are not digitally or not widely digitally delicate. Since the set of primes not digitally delicate is contained within the set of primes not widely digitally delicate, perhaps it is easier to show that there are an infinite number of primes not widely digitally delicate, or even a positive proportion of such primes. However, we have not made progress in this regard, and expect that methods other than those used in this dissertation would be necessary to establish such a result.

In [10], the existence of infinitely many *digitally durable* composite numbers n was established, that is, composite n satisfying the property that if any digit of n is replaced by a different digit, then the resulting number is composite. This easily follows from the methods of Erdős [5]. Extending this idea to the leading 0's of n, we define *widely digitally durable* composite numbers in the natural way.

Definition 2.5. A composite number n is *widely digitally durable* if n has the property that if any digit of n, including any of its infinitely many leading 0's, is replaced by a different digit, then the resulting number is composite.

It is not difficult to show that the approach in this dissertation also leads to the following result regarding such composite numbers.

Theorem 2.6. *There is a positive proportion of composite numbers that are widely digitally durable in base 10.*

Proof. Take $A \pmod M$ as in the proof of Theorem 1.3 and pick any prime r not dividing M. Let A' be the unique solution modulo $r \cdot M$ to the system

$$x \equiv A \pmod M, \qquad x \equiv 0 \pmod r.$$

Thus any number m satisfying $m \equiv A' \pmod{r \cdot M}$ has both the property that m is composite as well as the property that increasing any digit of m, including any of its infinitely many leading 0's, results in a number divisible by some prime dividing M.

The proof proceeds similarly to that in Section 2.2. Let K be a large integer. Our goal is to estimate the number of digitally durable composites d with $d \equiv A' \pmod{rM}$ and with d having $\leq K$ digits. Observe that the number of digit changes for such d is at most $9K$. We have that $d + \delta \cdot 10^j$, for $0 \leq j < K$ and $\delta \in \{0, 1, 2, \ldots, 8, 9\}$, is divisible by a prime dividing rM. For $d > rM$ and for $0 \leq j < K$ and $\delta \in \{0, 1, 2, \ldots, 8, 9\}$, we deduce then that $d + \delta \cdot 10^j$ is composite. We extend this to the $9K$ more numbers $d + \delta \cdot 10^j$ where $0 \leq j < K$ and $\delta \in \{-9, -8, \ldots, -2, -1\}$.

We continue as in Section 2.2 with the ideas of P. Erdős to dispense with most of these $9K$ possibilities by considering composites d only in residue classes modulo some primes for which 10 has small order. To be more precise, suppose k_0 is the smallest value of the order of 10 modulo a prime divisor of rM. Fix $\varepsilon > 0$, and let $K_0 = K_0(\varepsilon)$ be a positive integer to be specified later. For each integer $c \in (k_0, K_0]$, we choose the prime q_c as in Section 2.2 so that 10 has order c modulo q_c. Since the order of 10 modulo primes dividing rM are $\le k_0$, no q_c divides rM. We restrict our attention to primes $c \in (k_0, K_0]$ and again define for $\delta \in \{-9, -8, \cdots, -2, -1\}$ the set

$$\mathcal{Q}_\delta = \{c \in (k_0, K_0] : c \text{ prime}, c \equiv \delta \pmod{11}\}.$$

Fix, as before,

$$\mathcal{Q} = \bigcup_{\delta \in \{-9,-8,\ldots,-1\}} \mathcal{Q}_\delta, \qquad M' = \prod_{\delta \in \{-9,-8,\ldots,-1\}} \prod_{c \in \mathcal{Q}_\delta} q_c \qquad \text{and} \qquad W = MM'.$$

For each $\delta \in \{-9, -8, \ldots, -2, -1\}$, we consider

$$d \equiv -\delta \pmod{\prod_{c \in \mathcal{Q}_\delta} q_c}.$$

By the Chinese Remainder Theorem, there is a $B \in \mathbb{Z}$ such that these 9 congruences, one for each $\delta \in \{-9, -8, \ldots, -2, -1\}$, are equivalent to a single congruence $d \equiv B \pmod{M'}$. As a consequence, we have that if $d \equiv B \pmod{M'}$ and $\delta \in \{-9, -8, \ldots, -2, -1\}$, then for every nonnegative integer k that is divisible by a $c \in \mathcal{Q}_\delta$, we have $d + \delta \cdot 10^k$ is divisible by the prime q_c. Thus, with fixed $d \equiv B \pmod{M'}$ and fixed $\delta \in \{-9, -8, \ldots, -2, -1\}$, an inclusion-exclusion argument shows that the number of integers $j \in (0, K]$ with $d + \delta \cdot 10^j$ relatively prime to M' is

$$\le K \prod_{c \in \mathcal{Q}_\delta} \left(1 - \frac{1}{c}\right) + O\left(2^{K_0}\right). \tag{2.3}$$

We take $K_0 = K_0(\varepsilon)$ so that for K sufficiently large, the expression in (2.3) is $< \varepsilon K$, which is possible since $\sum^*_{c > k_0} 1/c$ diverges where the $*$ indicates the sum is over primes $c \equiv \delta \pmod{11}$.

Since $\gcd(rM, M') = 1$, the numbers d which are A' modulo rM and B modulo M' correspond to the primes in a single congruence class, say w, modulo $W = rMM'$. We now have that if $d \equiv w \pmod{W}$, then for all but $< 9\varepsilon K$ choices of $0 \leq j < K$ and $\delta \in \{-9, -8, \ldots, -2, -1\} \cup \{0, 1, 2, \ldots, 8, 9\}$, the number $d + \delta \cdot 10^j$ is divisible by a prime dividing W. Furthermore, the $< 9\varepsilon K$ choices for $\delta \cdot 10^j$ for which $d + \delta \cdot 10^j$ is not divisible by a prime dividing W are such that $\delta \in \{-9, -8, \ldots, -2, -1\}$ and j is free of prime factors from $\mathcal{Q}_\delta$. Let H denote this set of $\delta \cdot 10^j$ with $\delta \in \{-9, -8, \ldots, -2, -1\}$ and integers $j \in (0, K)$ free of prime factors from $\mathcal{Q}_\delta$. Note that $|H|$, the size of H, is bounded above by $9\varepsilon K$.

Now there are at least $10^K/W - \pi(10^K)$ composite numbers d up to 10^k satisfying $d \equiv w \pmod{W}$. For each of the numbers $h \in H$, the number of composite d so that $d + h$ is prime is at most $\pi(10^K)$. Thus the number of composites $d \equiv w \pmod{W}$ so that $d + \delta \cdot 10^k$ is composite for all $\delta \cdot 10^k = h \in H$ is at least

$$\frac{10^K}{W} - (9\epsilon K + 1)\pi(10^{k+1}) \geq \frac{10^K}{W} - (9\epsilon K + 1)\frac{10^K}{\log(10^K)}\left(1 + \frac{1.2762}{\log(10^K)}\right)$$
$$> \frac{10^K}{W} - \frac{2(9\epsilon K + 1)10^K}{K\log(10)} > \frac{10^K}{W} - 9\epsilon \cdot 10^K - \frac{10^K}{K}.$$

Taking $\epsilon < 1/(18W)$, we then obtain that the number of such composites d is at least

$$> \frac{10^K}{W} - \frac{10^K}{2W} - \frac{10^K}{K}.$$

Taking K sufficiently large, we see that there are a positive proportion of composites $d \leq x = 10^K$ with $d \equiv w \pmod{W}$ that are digitally durable. As these composites satisfy $d \equiv A \pmod{M}$, we deduce that a positive proportion of composites up to 10^K are widely digitally durable. As a positive proportion of composites up to 10^K is still a positive proportion of composites up to 10^{K+1}, we can see that the restriction of x to the form 10^K can be eliminated and there is a uniform lower bound on the proportion of composites up to x, for x large, that are widely digitally durable. $\square$

The proof of the analogue to Theorem 2.6 follows similarly in bases b where suitable coverings and congruence classes $A \pmod{M}$ have been found that allow for

increasing the digits of a number, but these methods do not hold for an arbitrary base.

Beyond the question of digit changing, one can also ask instead about inserting a digit. In [10], infinitely many composite numbers n were shown to have the property that if an arbitrary digit is inserted in n or before or after n, then the resulting number is also composite. This leads to several questions. Are there infinitely many primes p or a positive proportion of primes p such that if an arbitrary digit is inserted in p or before or after p, then the resulting number is composite? A list of such primes in base 10 is accessible through [28], but it is not known if the list is infinite. Do a positive proportion of primes have this property? What about the analogous question with leading 0's? We do not know the answers to these questions and expect that methods different than those used in this dissertation are required to establish such a result.

Chapter 3

Irreducibility criteria based on degree for polynomials with non-negative coefficients

3.1 Preliminary results

We begin with a few results that both motivate the steps we take and help establish a useful result.

Lemma 3.1. *Fix an integer $b > 1$. Let $f(x)$ be a polynomial with non-negative integer coefficients such that $f(b)$ is prime. If $f(x)$ is reducible, then $f(x)$ has a non-real root in the disc $\mathfrak{D}_b = \{z \in \mathbb{C} : |b - z| \leq 1\}$.*

Proof. Assume that $f(x)$ is reducible. Then $f(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ are in $\mathbb{Z}[x]$, have positive leading coefficients, and are not identically ± 1. Since $f(b)$ is prime, we may take, without loss of generality, $g(b) = \pm 1$ and $h(b) = \pm p$. Let c be the leading coefficient of $g(x)$, and denote its roots including multiplicity $\beta_1, ..., \beta_r$. Thus, the degree of $g(x)$ is r and we have

$$1 = |g(b)| = |c| \prod_{j=1}^{r} |b - \beta_j| \geq \prod_{j=1}^{r} |b - \beta_j|.$$

Thus, we conclude that at least one of the roots of $g(x)$, and hence of $f(x)$, is in $\mathfrak{D}_b$. The lemma then follows when we recall that $f(x)$ has no positive real roots since it has non-negative coefficients. □

One example of the usefulness of Lemma 3.1 can be found in the following lemma, which we use extensively in the proof of Theorem 1.4.

Lemma 3.2. *Let n be a positive integer. A complex number $\alpha = re^{i\theta}$ with $r > 0$ and $0 < \theta < \pi/n$ cannot be a root of a non-zero polynomial with non-negative integer coefficients and degree $\leq n$.*

Proof. Let $f(x) = \sum_{j=0}^{s} a_j x^j$ be a non-zero polynomial in $\mathbb{Z}[x]$ of degree s with each $a_j \geq 0$ and $s \leq n$. By way of contradiction, assume $\alpha = re^{i\theta}$ is a root of $f(x)$ with $r > 0$ and $0 < \theta < \pi/n$. Observe that α has a positive imaginary part. Since the complex conjugate of α is also a root of $f(x)$, we see that $s \geq 2$. For $1 \leq k \leq n$, we have $0 < k\theta < \pi$, so

$$\mathrm{Im}(\alpha^k) = r^k \sin(k\theta) > 0 \quad \text{for } 1 \leq k \leq n.$$

Since $f(x)$ has non-negative coefficients with $\deg f = s \leq n$, and α has positive imaginary part, we have

$$\mathrm{Im}(f(\alpha)) \geq \mathrm{Im}(\alpha^s) > 0,$$

contradicting the fact that α is a root of $f(x)$. □

Having established Lemmas 3.1 and 3.2, a motivating idea throughout the rest of this chapter is to replace the disk $\mathfrak{D}_b$ in Lemma 3.1 with a different region such that if $\alpha = re^{i\theta}$ is in this region, then $|\theta|$ is bounded above by a small number. This combined with Lemma 3.2 will give sharp bounds, $D_4(b)$, such that if $f(x)$ is a polynomial with non-negative integer coefficients with $f(b)$ prime for integers $b \geq 2$ and if the degree of $f(x)$ is $\leq D_4(b)$, then $f(x)$ must be irreducible, as discussed in Section 3.3.

3.2 A root bounding function

For a given integer $b \geq 5$ and $n \in \{3, 4, 6\}$, our main goal is to establish the bounds $D_n(b)$ in Theorem 1.4. In this section we introduce certain rational functions that will give us information about the location of possible roots of $f(x)$ assuming $f(x)$ is

reducible. While better rational functions can be chosen for small b, as in [4], we will make choices to simplify the results for the purposes of this dissertation.

Recall that $\Phi_n(x)$ denotes the nth cyclotomic polynomial, and let $\zeta_n = e^{2\pi i/n}$. Fix an integer $b \geq 5$, and let $f(x)$ be a non-constant polynomial with non-negative integer coefficients such that $f(b)$ is prime. Suppose $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are in $\mathbb{Z}[x]$, have positive leading coefficients, and are not identically ± 1. Since $f(b)$ is prime, we may take, without loss of generality, $g(b) = \pm 1$ and $h(b) = \pm f(b)$. Using the ideas of [9], we want to show that either $g(x)$ has a root in common with one of

$$\begin{aligned}
\Phi_3(x-b) &= x^2 - (2b-1)x + b^2 - b + 1, \\
\Phi_4(x-b) &= x^2 - 2bx + b^2 + 1, \\
\Phi_6(x-b) &= x^2 - (2b+1)x + b^2 + b + 1,
\end{aligned}$$

or $g(x)$ has roots in a certain region $\mathcal{R}_b$ to be defined shortly.

We define

$$\mathcal{F}_b(z) = \frac{\mathcal{N}_b(z)}{\mathcal{D}_b(z)}, \tag{3.1}$$

where

$$\mathcal{N}_b(z) = \ (|b + \zeta_3 - z||b + \overline{\zeta_3} - z|)^2 (|b + i - z||b - i - z|)^2 (|b + \zeta_6 - z||b + \overline{\zeta_6} - z|)^2$$

and

$$\mathcal{D}_b(z) = \ |b - z|^{16}.$$

In the notation of [4], this amounts to choosing

$$(e_2(b), e_3(b), e_4(b), e_6(b), d(b)) = (0, 1, 1, 1, 1),$$

but since our choice is constant we have simplified the presentation somewhat.

Setting $z = x + iy$, direct computations show that the expressions in $\mathcal{N}_b$ and $\mathcal{D}_b$ simplify to

$$\begin{aligned}(|b+\zeta_3-z||b+\overline{\zeta_3}-z|)^2 &= y^4+(2(x-b)^2+2(x-b)-1)y^2\\ &\quad +((x-b)^2+x-b+1)^2,\end{aligned}$$

$$(|b+i-z||b-i-z|)^2 = y^4+(2(x-b)^2-2)y^2+((x-b)^2+1)^2,$$

$$\begin{aligned}(|b+\zeta_6-z||b+\overline{\zeta_6}-z|)^2 &= y^4+(2(x-b)^2-2(x-b)-1)y^2\\ &\quad +((x-b)^2-(x-b)+1)^2,\end{aligned}$$

and

$$|b-z|^2 = y^2+(x-b)^2.$$

Notice that each one of these expressions is in $\mathbb{Z}[b, x, y^2]$. Thus, $\mathcal{N}_b(z)$ and $\mathcal{D}_b(z)$ are in $\mathbb{Z}[b, x, y^2]$, making $\mathcal{F}_b(z)$ a rational function in b, x, and y^2. Moreover, we observe that for each integer $b > 2$, the polynomial

$$\mathcal{P}_b(x, y) = \mathcal{D}_b(x + iy) - \mathcal{N}_b(x + iy) \tag{3.2}$$

can be written as

$$\mathcal{P}_b(x, y) = \sum_{j=0}^{8} a_j(b, x)y^{2j} \tag{3.3}$$

where each $a_j(b, x)$ is an integer polynomial in b and x. We write $g(x)$ in the form

$$g(x) = c\prod_{j=1}^{m}(x-\beta_j),$$

where c is the leading coefficient of $g(x)$ and $\beta_1, ..., \beta_m$ are the roots of $g(x)$. Since we have $f(x) = g(x)h(x)$, the β_j are also roots of $f(x)$. It can be shown, as is shown in more generality in [4], that

$$\frac{|g(b+\zeta_3)g(b+\overline{\zeta_3})|^2|g(b+i)g(b-i)|^2|g(b+\zeta_6)g(b+\overline{\zeta_6})|^2}{|g(b)|^{16}}$$

and

$$\frac{1}{c^4}\prod_{j=1}^{m}\mathcal{F}_b(\beta_j)$$

are equal. We denote this common value by $V = V_b(g)$.

Since each of $g(b+\zeta_3)g(b+\overline{\zeta_3})$, $g(b+i)g(b-i)$, and $g(b+\zeta_6)g(b+\overline{\zeta_6})$ is a symmetric polynomial in the roots of an irreducible monic quadratic in $\mathbb{Z}[x]$, we conclude that each of these expressions are themselves integers. Furthermore, $g(b) = \pm 1$. Thus, by looking at the first expression for V, either $V = 0$ or $V \in \mathbb{Z}^+$. In the case that $V = 0$, we see from either expression for V that $g(b+\zeta_3)g(b+\overline{\zeta_3})$, $g(b+i)g(b-i)$, or $g(b+\zeta_6)g(b+\overline{\zeta_6})$ is zero. This happens precisely when $g(x)$ is divisible by at least one of $\Phi_3(x-b)$, $\Phi_4(x-b)$, or $\Phi_6(x-b)$, so that if one of these shifted cyclotomic polynomials is not a factor of $g(x)$, we have $V \in \mathbb{Z}^+$. Observe that $\mathcal{F}_b(z)$ is a non-negative real number for all $z \in \mathbb{C}$. By looking at the product in the second expression for V, we see that if $V \neq 0$, then $\mathcal{F}_b(\beta_j) \geq 1$ for at least one value of $j \in \{1, ..., m\}$. Said in another way, if $V \neq 0$, then there is a root β_j of $g(x)$, and thus of $f(x)$, such that $\mathcal{F}_b(\beta_j) \geq 1$.

Summarizing the above ideas, given only that $g(x) \in \mathbb{Z}[x]$, $g(x) \not\equiv \pm 1$, and $g(b) = \pm 1$, we have shown that either $g(x)$ is divisible by at least one of $\Phi_3(x-b)$, $\Phi_4(x-b)$, and $\Phi_6(x-b)$, or $g(x)$ has a root β in the region

$$\mathcal{R}_b = \{z \in \mathbb{C} : F_b(z) \geq 1\}. \tag{3.4}$$

In the latter case, we will use an analysis of the region $\mathcal{R}_b$ in the complex plane to obtain important information about the location of β. For an illustration of $\mathcal{R}_b$, Figure 3.1 depicts the region $\mathcal{R}_5$.

While analyzing the region $\mathcal{R}_b$, we will sometimes refer to points (x, y) in $\mathcal{R}_b$. This is to be interpreted as the point $z = x + iy$ in the complex plane in $\mathcal{R}_b$. To further help analyze $\mathcal{R}_b$, we consider $\mathcal{P}_b(x, y)$ defined in equations (3.2) and (3.3).

The definition of $\mathcal{D}_b(z)$ implies that $\mathcal{D}_b(z) > 0$ for all complex $z \neq b$. Thus

$$\mathcal{F}_b(x+iy) \geq 1 \quad \text{and} \quad \mathcal{P}_b(x,y) \leq 0$$

are equivalent for $z \neq b$, and $\mathcal{F}_b(x+iy) = 1$ and $\mathcal{P}_b(x,y) = 0$ are equivalent for $z \neq b$. Note that $\mathcal{P}_b(b,0) = \mathcal{D}_b(b) - \mathcal{N}_b(b) = 0 - 1 = -1$. Therefore, the $z \in \mathbb{C}$ such that $\mathcal{F}_b(z) = 1$ correspond exactly to the points (x,y) where $\mathcal{P}_b(x,y) = 0$.

The following lemma corresponds to [9, Lemma 2], and the variation [4, Lemma 3.1].

Lemma 3.3. *Fix an integer $b \geq 2$. Then there exist real numbers $a_0 = a_0(b)$, $a_1 = a_1(b)$, and a non-negative real-valued function $\rho_b(x)$ defined on the interval $I_b = [b - a_0, b + a_1]$ such that:*

(i) $\mathcal{P}_b(x,y) \neq 0$ *for all* $x \notin I_b$ *and* $y \in \mathbb{R}$.

(ii) $\mathcal{P}_b(x, \rho_b(x)) = 0$ *for all* $x \in I_b$.

(iii) $\rho_b(b - a_0) = 0$ *and* $\rho_b(b + a_1) = 0$.

(iv) *The function $\rho_b(x)$ is continuously differentiable on the interior of I_b and is continuous on I_b.*

(v) *If x and y are real numbers for which $\mathcal{P}_b(x,y) \leq 0$, then $x \in I_b$ and $|y| \leq \rho_b(x)$.*

In view of the above lemma, complex numbers of the form $x + i\rho_b(x)$ are boundary points of $\mathcal{R}_b$, which are on or above the real axis. Since $\mathcal{P}_b(x,y)$ is a polynomial in y^2 with coefficients in $\mathbb{Z}[b,x]$, the region $\mathcal{R}_b$ is symmetric about the real axis. Thus, the points $x - i\rho_b(x)$ are boundary points of $\mathcal{R}_b$ which lie on or below the real axis. The points $b - a_0$ and $b + a_1$ are boundary points on the real axis.

A proof of Lemma 3.3 in more generality can be found in [4, Lemma 3.1]. In that proof, Cole et al. reduce the dependence on b to strictly a dependence on previously defined exponents $e_2(b)$, $e_3(b)$, $e_4(b)$, $e_6(b)$, and $d(b)$. They then use Sturm sequences

on the resulting polynomials in x to prove the lemma. One can verify computationally that the desired properties hold for our choice of $(e_2, e_3, e_4, e_6, d) = (0, 1, 1, 1, 1)$ when $b \geq 5$, with $a_0 = 1.522009\ldots$ and $a_1 = 1.522009\ldots$. Thus, the lemma follows.

In the next section we will use Lemma 3.3 to prove irreducibility criteria based on the degree of $f(x)$.

3.3 Irreducibility criteria based on degree

For the remainder of the chapter, we set for $n \in \{3, 4, 6\}$ and $b \in \mathbb{Z}^+$ the values

$$\theta_n = \theta_n(b) = \arg(b + \zeta_n) \quad \text{and} \quad D_n = D_n(b) = \left\lfloor \frac{\pi}{\theta_n} \right\rfloor.$$

Because D_n features prominently in what follows, we explain here how the following lemma is a consequence of [20, Corollary 3.12] which states that the only rational values of $\cos(\pi r)$ with $r \in \mathbb{Q}$ are 0, $\pm 1/2$, and ± 1.

Lemma 3.4. *Let $b \in \mathbb{Z}$ be greater than 2 and let $n \in \{3, 4, 6\}$. Then*

$$\frac{\pi}{\theta_n} \notin \mathbb{Z}.$$

Proof. Letting $r = \arg(b + \zeta_n)/\pi$, it suffices to show $r \notin \mathbb{Q}$. Observe that for $n \in \{3, 4, 6\}$ we have

$$\arg(b + \zeta_n) = \arctan(x) \quad \text{where} \quad x \in \left\{ \frac{\sqrt{3}}{2b-1}, \frac{1}{b}, \frac{\sqrt{3}}{2b+1} \right\}.$$

In each case, we have $\sin^2(\arctan(x)) = x^2/(x^2+1) \in \mathbb{Q}$, and hence

$$\cos(2\pi r) = \cos(2\arg(b + \zeta_n)) = 1 - 2\sin^2(\arg(b + \zeta_n)) \in \mathbb{Q}.$$

By Corollary 3.12 in [20], we deduce that if $r \in \mathbb{Q}$ then $\cos(2\arg(b+\zeta_n))$ is an element of $\{0, \pm 1/2, \pm 1\}$. One checks that $\arg(3 + \zeta_n) < \pi/6$ for each $n \in \{3, 4, 6\}$. Since $\arg(b+\zeta_n)$ decreases to 0 as b increases, we see that $\cos(2\arg(b+\zeta_n)) \notin \{0, \pm 1/2, \pm 1\}$ and the lemma follows. □

From Lemma 3.4, we obtain

$$D_n = \left\lfloor \frac{\pi}{\theta_n} \right\rfloor \neq \frac{\pi}{\arg(b+\zeta_n)} \quad \text{for } b > 2 \text{ and } n \in \{3, 4, 6\}. \tag{3.5}$$

One goal of this section involving D_n is to establish the following theorem.

Theorem 3.5. *Let $b \geq 5$ be an integer and $D_4 = \lfloor \pi / \arg(b+\zeta_4) \rfloor$. Let $f(x)$ be a polynomial with non-negative integer coefficients such that $f(b)$ is prime. If $\deg f(x) \leq D_4$, then $f(x)$ is irreducible.*

While we will establish several generalizations of Theorem 3.5, the principle generalization being Theorem 1.4, we begin with Theorem 3.5 because it is the product of a lengthy history in the literature. Its original predecessor appears as part of [7, Theorem 8], where Filaseta showed that the result above holds for all $b \geq 2$ when D_4 is replaced by the value $\lfloor \pi / \arcsin(1/b) \rfloor$. The values $D_4(b)$ and $\lfloor \pi / \arcsin(1/b) \rfloor$ usually coincide, but for some b, e.g., values b that appear as the denominator of an odd convergent to the simple continued fraction for π, we have $D_4(b) = \lfloor \pi / \arcsin(1/b) \rfloor + 1$. Thus Theorem 3.5 is a sharpening of that aspect of [7, Theorem 8]. Later, in [4], Theorem 3.5 was established for integers $2 \leq b \leq 20$, so we need only consider $b > 20$. However, the methods discussed here apply to all $b \geq 5$.

Proof. We begin by showing that if $\deg f(x) \leq D_4$ in Theorem 3.5, then $f(x)$ is irreducible. Recall the setup we have been using. That is, suppose that $f(x)$ is reducible and write $f(x) = g(x)h(x)$ where both $g(x)$ and $h(x)$ are in $\mathbb{Z}[x]$, $g(x) \not\equiv \pm 1$, $h(x) \not\equiv \pm 1$, and both $g(x)$ and $h(x)$ have positive leading coefficients. Furthermore, without loss of generality, we suppose that $g(b) = \pm 1$. In Section 3, we established that either $g(x)$ has a root in common with at least one of $\Phi_3(x-b)$, $\Phi_4(x-b)$, and $\Phi_6(x-b)$, or $g(x)$ has a root $\beta = re^{i\theta} \in \mathcal{R}_b$ where $\mathcal{R}_b$ is defined as in (3.4). We also define $\mathcal{P}_b(x, y)$ as in (3.2).

We continue in two steps. First, we show that $g(x)$ cannot share a root in common with any one of $\Phi_3(x-b)$, $\Phi_4(x-b)$, and $\Phi_6(x-b)$ using Lemma 3.2. Second, we

will bound $|\theta|$ using Lemma 3.3, then use Lemma 3.2 to show that $g(x)$ cannot have a root in $\mathcal{R}_b$, giving a contradiction.

For the first step, suppose $g(x)$ has a root $\beta = re^{i\theta} = b + \zeta_n$ where $n \in \{3, 4, 6\}$. Then we have $\theta = \theta_n = \arg(b + \zeta_n)$. To apply Lemma 3.2, we prove the following lemma.

Lemma 3.6. *Let $b \geq 4$ be an integer and D_4 be as in Theorem 3.5. Then*

$$\arg(b + \zeta_n) < \pi/D_4$$

for all $n \in \mathbb{N}$.

Proof. For $n \in \{1, 2\}$ and $n \geq 4$, the inequality

$$\arg(b + \zeta_n) \leq \arg(b + \zeta_4) \tag{3.6}$$

is easily verified for all $b \geq 4$. For $n = 3$, we show that (3.6) also holds for $b \geq 4$. Observe that

$$\arg(b + \zeta_3) = \arctan\left(\frac{\sqrt{3}/2}{b - 1/2}\right) \qquad \text{and} \qquad \arg(b + \zeta_4) = \arctan\left(\frac{1}{b}\right).$$

Thus, for $n = 3$ and $b \geq 4$, we want

$$\arctan\left(\frac{\sqrt{3}/2}{b - 1/2}\right) \leq \arctan\left(\frac{1}{b}\right),$$

which holds if and only if

$$\frac{\sqrt{3}/2}{b - 1/2} \leq \frac{1}{b}.$$

The latter inequality holds for $b \geq 3.74$. Thus, (3.6) holds for all $b \geq 4$ and $n \geq 1$. So for $b \geq 4$ and all $n \in \mathbb{N}$, we deduce that

$$\arg(b + \zeta_n) \leq \arg(b + \zeta_4) = \frac{\pi}{\pi/\arg(b + \zeta_4)} < \frac{\pi}{\lfloor \pi/\arg(b + \zeta_4) \rfloor} = \frac{\pi}{D_4}, \tag{3.7}$$

where the strict inequality follows from (3.5). Thus the lemma follows. □

By Lemma 3.2, since $0 < \arg(b+\zeta_n) < \pi/D_4$, any polynomial with non-negative integer coefficients with degree $\leq D_4$ cannot have a root whose angle is $\arg(b+\zeta_n)$. Thus, with $f(x)$ as in Theorem 3.5 of degree $\leq D_4$, neither $f(x)$ nor the factor $g(x)$ of $f(x)$, can have a root in common with any one of $\Phi_3(x-b)$, $\Phi_4(x-b)$, and $\Phi_6(x-b)$. This completes the first step.

For the second step, we consider the region $\mathcal{R}_b$ and suppose that $g(x)$ has a root $\beta = re^{i\theta} \in \mathcal{R}_b$, where we suppose as we may that $r > 0$ and $\theta \in (0, \pi/2)$. Let L_b be the line that passes through $b+\zeta_4$ and the origin given by $y = x/b$. Figure 3.1 shows $\mathcal{R}_5$ with the line L_5. Observe that, by definition, for all $b \geq 5$, the region $\mathcal{R}_b$ will be the same region as $\mathcal{R}_5$ but shifted to be centered at $(b, 0)$. We claim that the line L_b, defined by $y = x/b$, lies completely above the region $\mathcal{R}_b$ for $b \geq 5$. We use a Sturm sequence to see that $P_5(x, x/5)$ has no real roots. Using Lemma 3.3 (ii) and (iv), we deduce that the line L_5 does not intersect the region $\mathcal{R}_5$. Using a Sturm sequence with $P_5(x, 1)$, we deduce similarly that the line $y = 1$ does not intersect the region $\mathcal{R}_5$. Since $\mathcal{R}_b$ is simply a horizontal translation of $\mathcal{R}_5$, we see that the line $y = 1$ lies strictly above $\mathcal{R}_b$ for $b \geq 5$. The lines $y = 1$ and L_b intersect at $b+\zeta_4$, that is, the point $(b, 1)$. The smaller angle between these two lines is $\arctan(1/b) \leq \arctan(1/5)$. It follows that, since the line L_5 lies strictly above the region $\mathcal{R}_5$, we have also that the line L_b lies strictly above the region $\mathcal{R}_b$.

Since $\beta = re^{i\theta} \in \mathcal{R}_b$ with $\theta \in (0, \pi/2)$, we have that

$$0 < \theta < \arg(b+\zeta_4) < \pi/D_4 \tag{3.8}$$

where the last inequality holds from Lemma 3.6. Thus by Lemma 3.2, $f(x)$, and therefore $g(x)$, cannot have a root in the region $\mathcal{R}_b$. This completes the second step and thus the proof of Theorem 3.5. □

We defer a discussion of the sharpness of the value D_4 until later, after we have established Theorem 1.4. The bound D_4 in Theorem 3.5 can be improved via The-

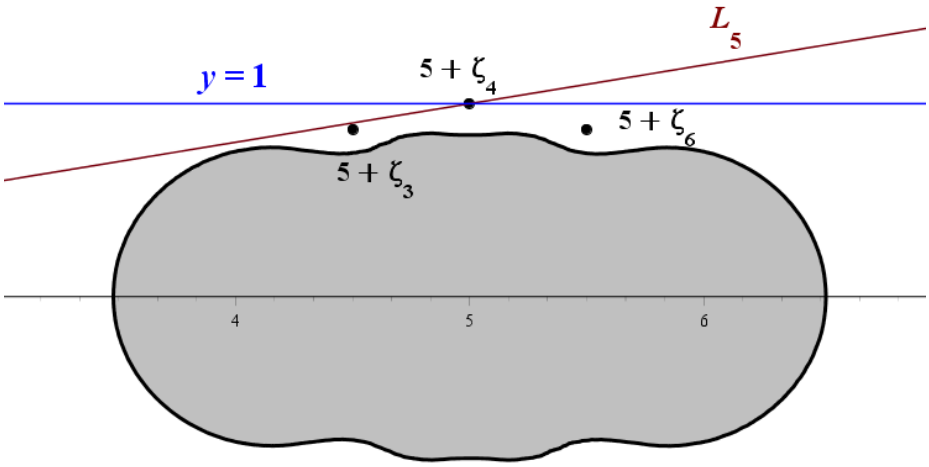

Figure 3.1 L_5 together with $\mathcal{R}_5$

orem 1.4 if one modifies the conclusion to allow for divisibility by one of the three cyclotomic polynomials $\Phi_3(x-b), \Phi_4(x-b)$, and $\Phi_6(x-b)$. To prove Theorem 1.4, we first show the following lemma.

Lemma 3.7. *Let b be an integer ≥ 5. Then*

$$D_4(b) < \frac{\pi}{\theta_4(b)} < D_3(b) < \frac{\pi}{\theta_3(b)} < D_6(b) < \frac{\pi}{\theta_6(b)} \quad \textit{for} \quad b \geq 5. \tag{3.9}$$

Proof. Note that for $n \in \{3,4,6\}$ and $b \geq 5$, the inequalities

$$D_n(b) = \left\lfloor \frac{\pi}{\theta_n(b)} \right\rfloor < \frac{\pi}{\theta_n(b)}$$

follow from (3.5). To establish the other inequalities, we write θ_n for $\theta_n(b)$ and define

$$\mathfrak{L}_n(b) = \frac{\pi}{\tan(\theta_n)} - 1 = \frac{\pi \operatorname{Re}(b+\zeta_n)}{\operatorname{Im}(b+\zeta_n)} - 1$$

and

$$\mathfrak{U}_n(b) = \frac{\pi}{\theta_n} = \frac{\pi}{\arctan\left(\operatorname{Im}(b+\zeta_n) / \operatorname{Re}(b+\zeta_n)\right)}.$$

Recall that

$$\operatorname{Re}(b+\zeta_n) = b + \cos(2\pi/n) \quad \text{and} \quad \operatorname{Im}(b+\zeta_n) = \sin(2\pi/n).$$

Thus, one can verify that $\mathfrak{L}_n(b)$ and $\mathfrak{U}_n(b)$ are real, differentiable functions of b for $b \geq 5$. Using (3.5), and since $x < \tan(x)$ for $x \in (0, \pi/2)$, we have

$$\mathfrak{L}_n(b) < D_n(b) < \mathfrak{U}_n(b) \qquad \text{for } b \in \mathbb{Z} \text{ and } b \geq 5. \tag{3.10}$$

Next for $n, m \in \{3, 4, 6\}$ define

$$\mathfrak{F}_{n,m}(b) = \mathfrak{L}_n(b) - \mathfrak{U}_m(b).$$

Then we obtain

$$\frac{d\mathfrak{F}_{n,m}}{db} = \frac{\pi}{\operatorname{Im}(b+\zeta_n)} - \frac{\pi \operatorname{Im}(b+\zeta_m)}{|b+\zeta_m|^2 \arctan\left(\operatorname{Im}(b+\zeta_m)/\operatorname{Re}(b+\zeta_m)\right)^2}.$$

Here, to simplify this derivative, and later, we use the Shafer-Fink ([11], [25]) inequalities

$$\frac{3x}{1+2\sqrt{1+x^2}} < \arctan(x) < \frac{\pi x}{1+2\sqrt{1+x^2}}, \quad \text{for } x > 0. \tag{3.11}$$

For this proof, we will only need the lower bound due to Shafer [25]. We deduce that

$$\begin{aligned}
\frac{d\mathfrak{F}_{n,m}}{db} &> \frac{\pi}{\operatorname{Im}(b+\zeta_n)} - \frac{\pi \operatorname{Im}(b+\zeta_m)}{|b+\zeta_m|^2} \cdot \left(\frac{1+2\sqrt{1+\left(\operatorname{Im}(b+\zeta_m)/\operatorname{Re}(b+\zeta_m)\right)^2}}{3\operatorname{Im}(b+\zeta_m)/\operatorname{Re}(b+\zeta_m)} \right)^2 \\
&= \frac{\pi}{\operatorname{Im}(b+\zeta_n)} - \frac{\pi \operatorname{Im}(b+\zeta_m)}{|b+\zeta_m|^2} \cdot \left(\frac{\operatorname{Re}(b+\zeta_m) + 2|b+\zeta_m|}{3\operatorname{Im}(b+\zeta_m)} \right)^2 \\
&> \frac{\pi}{\operatorname{Im}(b+\zeta_n)} - \frac{\pi \operatorname{Im}(b+\zeta_m)}{|b+\zeta_m|^2} \cdot \left(\frac{3|b+\zeta_m|}{3\operatorname{Im}(b+\zeta_m)} \right)^2 \\
&= \frac{\pi}{\operatorname{Im}(b+\zeta_n)} - \frac{\pi}{\operatorname{Im}(b+\zeta_m)} \\
&= \pi \left(\frac{1}{\sin(2\pi/n)} - \frac{1}{\sin(2\pi/m)} \right).
\end{aligned}$$

One then verifies from the above that $\mathfrak{F}_{3,4}(b)$ and $\mathfrak{F}_{6,3}(b)$ are increasing functions of b for $b > 6$. Since $\mathfrak{F}_{3,4}(7) > 0.4$ and $\mathfrak{F}_{6,3}(7) > 2.4$, for integers $b > 6$ we have

$$\mathfrak{U}_4(b) < \mathfrak{L}_3(b) < \mathfrak{U}_3(b) < \mathfrak{L}_6(b) < \mathfrak{U}_6(b). \tag{3.12}$$

One checks that (3.9) holds when $b = 5$ and $b = 6$. Thus, combining (3.5), (3.10), and (3.12), we deduce that (3.9) holds. □

We now improve Theorem 3.5 with Theorem 1.4 by allowing for $f(x)$ to be divisible by one or more of the cyclotomic polynomials $\Phi_3(x-b)$, $\Phi_4(x-b)$, or $\Phi_6(x-b)$. We restate Theorem 1.4 here for reference.

Theorem 1.4. *Fix an integer $b \geq 5$, and for $n \in \{3,4,6\}$ set*

$$D_n = D_n(b) = \left\lfloor \frac{\pi}{\arg(b+\zeta_n)} \right\rfloor \qquad \text{and} \qquad D = D(b) = \left\lfloor \frac{\pi}{\arctan\left(\frac{1732}{1000(2b+1)}\right)} \right\rfloor.$$

Let $f(x) \in Z[x]$ with non-negative coefficients and with $f(b)$ prime. If the degree of $f(x)$ is $\leq D_4$, then $f(x)$ is irreducible. Additionally, if the degree of $f(x)$ is $\leq D_3$ and $f(x)$ is reducible, then $f(x)$ is divisible by $\Phi_4(x-b)$ and not divisible by $\Phi_3(x-b)$ or $\Phi_6(x-b)$. Furthermore, in the case that $b > 26$, if the degree of $f(x)$ is $\leq D_6$ and $f(x)$ is reducible, then $f(x)$ is divisible by either $\Phi_4(x-b)$ or $\Phi_3(x-b)$ and not by $\Phi_6(x-b)$. Lastly, in the case that $b > 26$, if the degree of $f(x)$ is $\leq D$ and $f(x)$ is reducible, then $f(x)$ is divisible by $\Phi_4(x-b)$, $\Phi_3(x-b)$, or $\Phi_3(x-b)$.

Before proceeding to the proof, we note that Cole et al. have already established the portions of Theorem 1.4 that hold for $5 \leq b \leq 20$ as well as an analogous statement for D_4 regarding $b \in \{2,3,4\}$, which appears in [4, Theorem 4.2]. They accomplish this via the use of a different region $\mathcal{R}_b$ than we chose but which achieves the same result. In this sense, Theorem 1.4 can be viewed as an extension of [4, Theorem 4.2] to $b > 20$.

Proof. In addition to the inequalities in (3.9), we note that

$$D_6(b) = \left\lfloor \frac{\pi}{\arctan(\sqrt{3}/(2b+1))} \right\rfloor \leq \left\lfloor \frac{\pi}{\arctan(1732/(1000(2b+1)))} \right\rfloor = D(b).$$

Unlike (3.9), the above is not a strict inequality. When equality occurs is discussed in more detail after this proof.

Recall the proof of Lemma 3.3. We set

$$(e_2, e_3, e_4, e_6, d) = (0,1,1,1,1).$$

We define $\mathcal{F}_b(z)$ as in (3.1), $\mathcal{P}_b(x,y)$ as in (3.2), and $\mathcal{R}_b$ as in (3.4). In addition to $D_4 = D_4(b)$, $D_3 = D_3(b)$, $D_6 = D_6(b)$, and $D = D(b)$, we set for $b \in [5,26]$ the values $\vartheta = \vartheta(b) = \pi/D_3(b)$ and $m = m(b) = 1732/(1000(2b-1))$. For $b > 26$, we set $\vartheta = \vartheta(b) = \pi/D(b)$ and $m = m(b) = 1732/(1000(2b+1))$. We note that for each b, the number m is a rational number.

We consider the line $y = \tan(\vartheta)x$ or equivalently the points $x + i\tan(\vartheta)x$ in the complex plane. Using our choices for ϑ and m, we obtain for $b > 26$ that

$$\tan(\vartheta) = \tan\left(\frac{\pi}{\left\lfloor \frac{\pi}{\arctan(1732/(1000(2b+1)))} \right\rfloor}\right) > \tan\left(\arctan\left(\frac{1732}{1000(2b+1)}\right)\right) = m.$$

A calculation shows that $\tan(\vartheta) > m$ also holds for $b \in [5,26]$. So the line $y = mx$ lies strictly below the line $y = \tan(\vartheta)x$ for $x > 0$. Applying Lemma 3.3, we know that $\rho_b(b - a_0) = 0$ and that $\rho_b(x)$ is continuous. We claim that $y = mx$ lies entirely above the region $\mathcal{R}_b$ for $b > 26$. We use a Sturm sequence to verify that when $b = 27$, the polynomial $\mathcal{P}_{27}(x, m(27)x)$ has no real roots. Using Lemma 3.3 (ii) and (iv), we deduce that the line $y = m(27)x$ does not intersect the region $\mathcal{R}_{27}$. Using a Sturm sequence with $\mathcal{P}_{27}(x, 1732/2000)$, we deduce similarly that the line $y = 1732/2000$ does not intersect $\mathcal{R}_{27}$. Since $\mathcal{R}_b$ is simply a horizontal translation of $\mathcal{R}_{27}$, we see that the line $y = 1732/2000$ lies strictly above the region $\mathcal{R}_b$ for all $b \geq 27$. The lines $y = 1732/2000$ and $y = mx$ intersect at the point $(b + 1/2,\ 1732/2000)$. The smaller angle between these two lines is $\arctan(m(b))$, which is $\leq \arctan(m(27))$ for $b \geq 27$. It follows that, since the line $y = m(27)x$ lies strictly above the region $\mathcal{R}_{27}$, we have also that for $b \geq 27$, the line $y = m(b)x$ lies strictly above the region $\mathcal{R}_b$. For $b \in [5,26]$, we verify similarly with a Sturm sequence that $y = m(b)x$ lies strictly above the region $\mathcal{R}_b$.

We recall the set-up from Section 3.2. We suppose $f(x)$ is reducible and write $f(x) = g(x)h(x)$, where both $g(x)$ and $h(x)$ are in $\mathbb{Z}[x]$, $g(x) \not\equiv \pm 1$, $h(x) \not\equiv \pm 1$, and both $g(x)$ and $h(x)$ have positive leading coefficients. Furthermore, without loss of generality, we suppose that $g(b) = \pm 1$. In Section 3.2, we showed that either $g(x)$ has

a root in common with at least one of $\Phi_3(x-b)$, $\Phi_4(x-b)$, and $\Phi_6(x-b)$, or $g(x)$ has a root $\beta \in \mathcal{R}_b$. Since $f(x)$ has non-negative coefficients and the real numbers in $\mathcal{R}_b$ are positive, we know that $\beta \notin \mathbb{R}$. So take $\beta = \sigma + it$ such that $0 < t < m\sigma < \tan(\vartheta)\sigma$. Note the latter implies that we can alternatively write $\beta = re^{i\vartheta'}$, with $r > 0$ and $0 < \vartheta' < \vartheta$.

By Theorem 3.5, we have that $f(x)$ is irreducible if $\deg f(x) \leq D_4(b)$. We now turn to establishing the statements concerning D_3 and D_6. In order to apply Lemma 3.2, we observe that

$$0 < \vartheta' < \vartheta = \frac{\pi}{D_3} \quad \text{for} \quad b \in [5, 26]$$

and

$$0 < \vartheta' < \vartheta = \frac{\pi}{D} < \frac{\pi}{D_3} \quad \text{for} \quad b \geq 27.$$

For $b \geq 5$, we have from (3.9) that

$$\arg(b + \zeta_6) < \arg(b + \zeta_3) < \frac{\pi}{D_3}.$$

If $f(x)$ is reducible and $\deg f(x) \leq D_3$, we know that $f(x)$ cannot have a root in $\mathcal{R}_b$, since otherwise $f(x)$ has a root $\beta = re^{i\vartheta'} \in \mathcal{R}_b$, with $r > 0$ and $0 < \vartheta' < \pi/D_3$, contradicting Lemma 3.2. Similarly, since $\arg(b + \zeta_6) < \arg(b + \zeta_3) < \pi/D_3$, the polynomials $\Phi_3(x - b)$ and $\Phi_6(x - b)$ cannot be factors of $f(x)$, so $f(x)$ is divisible by $\Phi_4(x - b)$.

For $b > 26$, we have from (3.9) that $\arg(b + \zeta_6) < \pi/D_6$. Thus, we know that if $f(x)$ is reducible and the degree of $f(x)$ is $\leq D_6$, then from Lemma 3.2 and $0 < \vartheta' < \pi/D \leq \pi/D_6$ we obtain that $f(x)$ does not have a root in $\mathcal{R}_b$ and $f(x)$ is not divisible by $\Phi_6(x - b)$, so that $f(x)$ must be divisible by $\Phi_3(x - b)$ or $\Phi_4(x - b)$. Last, for $b > 26$, we have from Lemma 3.2 and $0 < \vartheta' < \pi/D$ that if $f(x)$ is reducible and the degree of $f(x)$ is $\leq D$, then $f(x)$ cannot have a root in $\mathcal{R}_b$, so that $f(x)$ is divisible by $\Phi_3(x - b), \Phi_4(x - b)$, or $\Phi_6(x - b)$. $\square$

The values D and D_6 coincide for finitely many values of b. They first differ when $b = 64$ and they last agree when $b = 9355$. These facts can be shown using the notation of Lemma 3.7, where

$$\mathfrak{U}_6(b) = \frac{\pi}{\theta_6} \quad \text{and thus} \quad D(b) = \left\lfloor \mathfrak{U}_6\left(\frac{500\sqrt{3}(2b+1)}{1732} - \frac{1}{2}\right)\right\rfloor.$$

To show these values differ when b is large, consider the derivative $d\mathfrak{U}_6/db$. Using (3.11), we have for $b \geq 2$ that

$$\begin{aligned}
\frac{d\mathfrak{U}_6}{db} &= \frac{\pi \operatorname{Im}(b+\zeta_6)}{|b+\zeta_6|^2 \arctan^2\left(\operatorname{Im}(b+\zeta_6)/\operatorname{Re}(b+\zeta_6)\right)} \\
&> \frac{\pi \operatorname{Im}(b+\zeta_6)}{|b+\zeta_6|^2} \cdot \left(\frac{1+2\sqrt{1+\left(\operatorname{Im}(b+\zeta_6)/\operatorname{Re}(b+\zeta_6)\right)^2}}{\pi \operatorname{Im}(b+\zeta_6)/\operatorname{Re}(b+\zeta_6)}\right)^2 \\
&= \frac{\pi \operatorname{Im}(b+\zeta_6)}{|b+\zeta_6|^2} \cdot \left(\frac{\operatorname{Re}(b+\zeta_6)+2|b+\zeta_6|}{\pi \operatorname{Im}(b+\zeta_6)}\right)^2 \\
&> \frac{\pi \operatorname{Im}(b+\zeta_6)}{|b+\zeta_6|^2} \cdot \left(\frac{2|b+\zeta_6|}{\pi \operatorname{Im}(b+\zeta_6)}\right)^2 = \frac{4}{\pi \operatorname{Im}(b+\zeta_6)} = \frac{8}{\pi\sqrt{3}} > 1.
\end{aligned}$$

We see then that $\mathfrak{U}_6(b)$ is increasing for $b \geq 2$ and, by the Mean Value Theorem, $\mathfrak{U}_6(b+1) > \mathfrak{U}_6(b) + 1$ for $b \geq 2$. Thus, to obtain $D(b) > D_6(b)$, it suffices to show that

$$\left(\frac{500\sqrt{3}(2b+1)}{1732} - \frac{1}{2}\right) - b > 1.$$

Solving, we see this inequality holds for $b > 34088$. One checks directly that for all integers $b \in (9355, 34088]$, we have $D(b) > D_6(b)$.

Via a generalization of the argument used by Filaseta in [7], we can show that the bounds D_3, D_4, and D_6 appearing in Theorem 1.4 are sharp, i.e., they are the largest values having the stated properties.

Theorem 3.8. *Let $b \geq 5 \in \mathbb{Z}$. For each $n \in \{3, 4, 6\}$, let $m_n \in \mathbb{Z}^+$, $m_n \geq D_n(b) + 1$. Then there are an infinite number of polynomials $f_n(x) \in \mathbb{Z}[x]$ of degree m_n with non-negative coefficients for which $f_n(b)$ is prime and $\Phi_n(x-b) \mid f_n(x)$.*

We note that this result has already been shown for D_4 in Lemma 3, Lemma 4 and Theorem 8 of [7]. The proof below reproduces those arguments with enough generalization to show the same result for D_3 and D_6.

Proof. Fix

$$\rho_3 = (b^2 - b + 1)^{1/2}, \quad \rho_4 = (b^2 + 1)^{1/2}, \quad \rho_6 = (b^2 + b + 1)^{1/2}$$

and note that for each $n \in \{3, 4, 6\}$ we have

$$\Phi_n(x - b) = (x - \kappa)(x - \lambda) \quad \text{where} \quad \kappa = \rho_n e^{i\theta_n}, \quad \lambda = \rho_n e^{-i\theta_n}.$$

Set $s_n = D_n(b) - 1$. Since $b \geq 5$, we have that s_n is non-negative. For $j \in \{-1, 0, 1, \ldots, s_n, s_n + 1\}$, define

$$c_{j,n} = \frac{\kappa^{s_n - j + 1} - \lambda^{s_n - j + 1}}{\kappa - \lambda}.$$

Observe that the numbers defined by $d_j = d_j(n) = c_{s_n+1-j,n}$ satisfy $d_0 = c_{s_n+1,n} = 0$, $d_1 = c_{s_n,n} = 1$ and

$$\begin{aligned} d_{j+2} = c_{s_n-j-1,n} &= (\kappa + \lambda)c_{s_n-j,n} - \kappa\lambda c_{s_n-j+1,n} \\ &= (\kappa + \lambda)d_{j+1} - \kappa\lambda d_j, \qquad \text{for } 0 \leq j \leq s_n. \end{aligned}$$

The above is a recursion relation for d_j with characteristic polynomial $\Phi_n(x - b)$. We deduce that $c_{j,n} \in \mathbb{Z}$ for each $j \in \{-1, 0, 1, \ldots, s_n, s_n + 1\}$ and each $n \in \{3, 4, 6\}$. Furthermore, setting

$$u_n(x) = \sum_{j=0}^{s_n} c_{j,n} x^j = \sum_{j=0}^{s_n} c_{s_n-j,n} x^{s_n-j} = \sum_{j=1}^{s_n+1} d_j x^{s_n+1-j},$$

we see that the above recursion implies

$$\Phi_n(x - b)u_n(x) = x^{s_n+2} - \frac{\kappa^{s_n+2} - \lambda^{s_n+2}}{\kappa - \lambda} x + \frac{\kappa^{s_n+1} - \lambda^{s_n+1}}{\kappa - \lambda} \kappa\lambda.$$

Then since $c_{j,n} = \rho_n^{s_n-j} \sin((s_n - j + 1)\theta_n)/\sin(\theta_n)$, we obtain

$$\Phi_n(x - b)u_n(x) = x^{s_n+2} - \rho_n^{s_n+1} \frac{\sin((s_n + 2)\theta_n)}{\sin(\theta_n)} x + \rho_n^{s_n+2} \frac{\sin((s_n + 1)\theta_n)}{\sin(\theta_n)}.$$

Recalling (3.5), we have

$$0 < (s_n+1)\theta_n = D_n\theta_n < (\pi/\theta_n)\cdot\theta_n = \pi < (s_n+2)\theta_n = D_n\theta_n + \theta_n < \pi + \theta_n < 2\pi.$$

We obtain that $\sin((s_n+2)\theta_n)$ is negative and $\sin((s_n+1)\theta_n)$ is positive, so that the coefficient of x and the constant term in $\Phi_n(x-b)u_n(x)$ are positive.

Taking m_n as in the statement of the theorem, observe that we have $m_n \geq s_n+2$. To obtain a polynomial of degree m_n, we define

$$h_n(x) = u_n(x)(x^{m_n-s_n-2} + x^{m_n-s_n-1} + \cdots + x + 1)$$

so that for an $n \in \{3,4,6\}$, $\Phi_n(x-b)h_n(x)$ is a polynomial of degree m_n having all non-negative coefficients. Then set

$$w_n(x) = (2b+1)h_n(x) + 1.$$

Since the coefficients of $\Phi_n(x-b)h_n(x)$ are non-negative and the coefficient for x is non-zero, the coefficient of x in $\Phi_n(x-b)h_n(x)$ must be at least 1. This implies that

$$\Phi_n(x-b)w_n(x) = (2b+1)\Phi_n(x-b)h_n(x) + \Phi_n(x-b)$$

has non-negative coefficients, as the least negative coefficient appearing in $\Phi_n(x-b)$ for each $n \in \{3,4,6\}$ is $-1-2b$ when $n=6$. Furthermore, the values

$$h_n(b) = \Phi_n(b-b)h_n(b) \quad \text{and} \quad w_n(b) = (2b+1)h_n(b)+1$$

are both positive and relatively prime. Thus every sufficiently large integer is of the form $\alpha_n h_n(b) + \gamma_n w_n(b)$ for some $\alpha_n, \gamma_n \in \mathbb{Z}^+$. In particular, for each $n \in \{3,4,6\}$ there are infinitely many primes p_n such that for some positive integers α_n, γ_n, we have $\alpha_n h_n(b) + \gamma_n w_n(b) = p_n$. Set

$$f_n(x) = \Phi_n(x-b)(\alpha_n h_n(x) + \gamma_n w_n(x)).$$

Then $f_n(x)$ has degree m_n, is reducible, has all non-negative coefficients, and is such that $f_n(b) = p_n$, a prime. Since there are infinitely many choices for the prime p_n,

we get that there are infinitely many choices for $f_n(x)$, completing the proof of the theorem. $\square$

The bounds in Theorem 3.5 and Theorem 1.4 can be generalized to an arbitrary degree if one allows for the possibility of $f(x)$ being divisible by some polynomial taken from a finite set of polynomials. To show this result, we first prove the following lemma.

Lemma 3.9. *Fix $\varepsilon \in (0,1)$ and $G \in \mathbb{Z}^+$. Let $\mathcal{W} = \mathcal{W}(\varepsilon, G)$ denote the set of $g(x) \in \mathbb{Z}[x]$ for which $|g(0)| = 1$, $\deg g(x) \in [1, G]$, and $|\alpha| \geq \varepsilon$ for each root $\alpha \in \mathbb{C}$ of $g(x)$. Then $\mathcal{W}$ is a finite set.*

Proof. Let $w(x) \in \mathcal{W}$, and set $n = \deg g$. The definition of $\mathcal{W}$ implies $n \leq G$. Let $\alpha_1, \ldots, \alpha_n$ denote the roots of $w(x)$, appearing to their multiplicity. Let a denote the leading coefficient of $w(x)$. Since $w(x) \in \mathcal{W}$, we obtain $|w(0)| = 1$ and, for each $j \in \{1, 2, \ldots, n\}$, we have $|\alpha_j| \geq \varepsilon$. Hence,

$$\varepsilon^G \leq \varepsilon^n \leq |\alpha_1|\,|\alpha_2| \cdots |\alpha_n| = \frac{|w(0)|}{|a|} = \frac{1}{|a|} \implies |a| \leq \frac{1}{\varepsilon^G}.$$

Furthermore, for each $j \in \{1, 2, \ldots, n\}$, we deduce

$$|\alpha_j| = \frac{|\alpha_1|\,|\alpha_2| \cdots |\alpha_n|}{|\alpha_1|\,|\alpha_2| \cdots |\alpha_{j-1}|\,|\alpha_{j+1}| \cdots |\alpha_{n-1}|\,|\alpha_n|} \leq \frac{1/|a|}{\varepsilon^{n-1}} \leq \frac{1}{|a|\varepsilon^{G-1}}.$$

As each coefficient of $w(x)$ after the leading coefficient is $\pm a$ times a sum of a product of distinct α_j, we see that the absolute value of each coefficient of $w(x)$ is bounded above by

$$\begin{aligned} |a|2^n \max\{1/(|a|\varepsilon^{G-1}), 1\}^n &\leq |a|2^G \max\{1/(|a|\varepsilon^{G-1}), 1\}^G \\ &\leq \frac{|a|2^G}{(|a|\varepsilon^{G-1})^G} + |a|2^G \\ &\leq \frac{2^G}{\varepsilon^{(G-1)G}} + \frac{2^G}{\varepsilon^G}. \end{aligned}$$

The lemma follows as we now see that the degree of $w(x)$ is bounded and the absolute value of each coefficient of $w(x)$ is bounded by a function depending only on the fixed numbers ε and G. $\square$

Theorem 3.10. *Let b and G be integers ≥ 2. Then there is a finite set $S = S(b, G)$ of polynomials in $\mathbb{Z}[x]$ such that, for all $f(x) \in \mathbb{Z}[x]$ with $f(x)$ having non-negative integer coefficients, $f(b)$ prime and $\deg f \leq G$, either $f(x)$ is irreducible or $f(x)$ is divisible by some polynomial $g(x) \in S$.*

Proof. It suffices to establish the theorem for $b \geq 2$ fixed and G sufficiently large, so we take G so that

$$b \sin(\pi/G) \in (0, 1).$$

Suppose $f(x) \in \mathbb{Z}[x]$ with $f(x)$ having non-negative integer coefficients, $f(b)$ prime, $\deg f \leq G$, and $f(x)$ reducible. Since $f(b)$ is prime, we have that $f(x) = g(x)h(x)$ with $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$, with $\deg g(x) \geq 1$, and with $g(b) = \pm 1$. Since the roots of $g(x)$ are roots of $f(x)$ and $\deg f(x) \leq G$, Lemma 3.2 implies that $g(x)$ cannot have any root $\alpha = re^{i\theta}$ with $r \geq 0$ and $0 < \theta < \pi/G$. One checks that the line passing through the origin with slope $\tan(\pi/G)$ is tangent to the circle centered at b of radius $b \sin(\pi/G)$. Taking $\varepsilon = b \sin(\pi/G) \in (0, 1)$ and $w(x) = g(x + b)$ in Lemma 3.9, we deduce that there are a finite number of possibilities for the factor $g(x)$ of $f(x)$. Taking S to be the set of these finitely many possibilities for $g(x)$, the theorem follows. $\square$

Bibliography

[1] A. S. Bang. "Taltheoretiske Undersøgelser". In: *Tidsskrift for Mat.* 4 (1886), pp. 70–80, 130–137.

[2] John Brillhart, Michael Filaseta, and Andrew Odlyzko. "On an irreducibility theorem of A. Cohn". In: *Canadian J. Math.* 33.5 (1981), pp. 1055–1059.

[3] John Brillhart et al. *Factorizations of* $b^n \pm 1$. Third. Vol. 22. Contemporary Mathematics. $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to high powers. American Mathematical Society, Providence, RI, 2002, pp. xcvi+236.

[4] Morgan Cole, Scott Dunn, and Michael Filaseta. "Further irreducibility criteria for polynomials with non-negative coefficients". In: *Acta Arith.* 175.2 (2016), pp. 137–181.

[5] Paul Erdős. "Solution to problem 1029: Erdos and the computer". In: *Mathematics Magazine* 52 (1979), pp. 180–181.

[6] Michael Filaseta. "A further generalization of an irreducibility theorem of A. Cohn". In: *Canad. J. Math.* 34.6 (1982), pp. 1390–1395.

[7] Michael Filaseta. "Irreducibility criteria for polynomials with nonnegative coefficients". In: *Canad. J. Math.* 40.2 (1988), pp. 339–351.

[8] Michael Filaseta, Carrie Finch, and Mark Kozek. "On powers associated with Sierpiński numbers, Riesel numbers and Polignac's conjecture". In: *Journal of Number Theory* 128 (July 2008), pp. 1916–1940.

[9] Michael Filaseta and Samuel Gross. "4959866698915122609810424451291 8". In: *J. Number Theory* 137 (2014), pp. 16–49.

[10] Michael Filaseta et al. "Composites that remain composite after changing a digit". In: *J. Comb. Number Theory* 2.1 (2010), 25–36 (2011).

[11] Arlington M. Fink. "Two inequalities". In: *Univ. Beograd. Publ. Elektrotehn. Fak. Ser. Mat.* 6 (1995), pp. 48–49.

[12] Joseph Foster, Jacob Juillerat, and Jeremiah Southwick. “The irreducibility of polynomials arising from the study of Fourier coefficients of powers of the Dedekind-eta function”. In: *Journal of Combinatorics and Number Theory* 10.3 (2018).

[13] Heine Halberstam and Hans Egon Richert. *Sieve methods*. London Mathematical Society Monographs, No. 4. Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London-New York, 1974, xiv+364 pp. (loose errata).

[14] Bernhard Heim, Florian Luca, and Markus Neuhauser. “Recurrence relations for polynomials obtained by arithmetic functions”. In: *Int. J. Number Theory* 15.6 (2019), pp. 1291–1303.

[15] Bernhard Heim and Markus Neuhauser. “Log-concavity of recursively defined polynomials”. In: *J. Integer Seq.* 22.1 (2019), Art. 19.1.5, 12.

[16] Bernhard Heim, Markus Neuhauser, and Florian Rupp. “Fourier coefficients of powers of the Dedekind eta function”. In: *Ramanujan J.* 48.1 (2019), pp. 1–11.

[17] Jackson Hopper and Paul Pollack. “Digitally delicate primes”. In: *J. Number Theory* 168 (2016), pp. 247–256.

[18] Dan Ismailescu and Peter Seho Park. “On pairwise intersections of the Fibonacci, Sierpiński, and Riesel sequences”. In: *J. Integer Seq.* 16.9 (2013), Article 13.9.8, 9.

[19] Murray S. Klamkin. “Problem 1029”. In: *Mathematics Magazine* 51 (1978), p. 69.

[20] Ivan Niven. *Irrational numbers*. The Carus Mathematical Monographs, No. 11. The Mathematical Association of America. Distributed by John Wiley and Sons, Inc., New York, N.Y., 1956, pp. xii+164.

[21] Ken Ono. *The web of modularity: arithmetic of the coefficients of modular forms and q-series*. Vol. 102. CBMS Regional Conference Series in Mathematics. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 2004, pp. viii+216. ISBN: 0-8218-3368-5.

[22] Georg Pólya and Gabor Szegő. *Aufgaben und Lehrsätze aus der Analysis. Band II: Funktionentheorie, Nullstellen, Polynome Determinanten, Zahlentheorie*. Vierte Auflage, Heidelberger Taschenbücher, Band 74. Springer-Verlag, Berlin-New York, 1971, xii+407 pp. (loose errata).

[23] Maruti Ram Murty. "Prime numbers and irreducible polynomials". In: *Amer. Math. Monthly* 109.5 (2002), pp. 452–458.

[24] Issai Schur. "Affektlose Gleichungen in der Theorie der Laguerreschen und Hermiteschen Polynome". In: *J Reine Angew. Math.* 165 (1931), pp. 52–58.

[25] Robert E. Shafer. "Problem E 1867". In: *Amer. Math. Monthly* 73 (1966), p. 309.

[26] Neil J. A. Sloane, ed. *The On-Line Encyclopedia of Integer Sequences*. URL: `https://oeis.org/A050249` (visited on 03/06/2019).

[27] Neil J. A. Sloane, ed. *The On-Line Encyclopedia of Integer Sequences*. URL: `https://oeis.org/A076336` (visited on 03/06/2020).

[28] Neil J. A. Sloane, ed. *The On-Line Encyclopedia of Integer Sequences*. URL: `https://oeis.org/A125001` (visited on 03/06/2020).

[29] Cameron L. Stewart. "On divisors of Lucas and Lehmer numbers". In: *Acta Math.* 211.2 (2013), pp. 291–314.

[30] Terence Tao. "A remark on primality testing and decimal expansions". In: *J. Aust. Math. Soc.* 91.3 (2011), pp. 405–413.

[31] Karl Zsigmondy. "Zur Theorie der Potenzreste". In: *Monatsh. Math. Phys.* 3.1 (1892), pp. 265–284.

Appendix A

Coverings for bases other than 10

For bases other than 10, we wish to establish the statement analogous to Theorem 1.3. To do so, we exhibit coverings of the integers corresponding to the following generalization of Lemma 2.2.

Lemma A.1. *Let $A, b \in \mathbb{Z}^+$, and for a prime p relatively prime to b let $c_b(p)$ be the multiplicative order of p mod b. For a fixed $\delta \in \{0, \ldots, b-1\}$, suppose we have distinct primes $p_1, \ldots, p_t$, each relatively prime to b, satisfying the following.*

(i) There exists a covering of the integers

$$k \equiv b_i \pmod{c_b(p_i)}, \quad 1 \leq i \leq t.$$

(ii) The number A satisfies each of the congruences

$$A \equiv -\delta \cdot b^{b_i} \pmod{p_i}, \quad 1 \leq i \leq t.$$

Then, for each $k \in \mathbb{Z}^+ \cup \{0\}$, the number

$$A + \delta \cdot b^k$$

is divisible by at least one of the primes p_i where $1 \leq i \leq t$.

The proof for Lemma A.1 is identical to that of Lemma 2.2. In the tables that follow, we have at times truncated the presentation of the congruences chosen so as to meet formatting guidelines. For example, in Table A.12 we have removed the columns with heading 'row' to allow for more horizontal space and have also shortened the

presentation of each residue class chosen. Whenever possible, each covering progresses roughly for some m from $k \equiv 0 \pmod{m}$ through $k \equiv m-1 \pmod{m}$. However, we have at times rearranged the rows in the interest of placing any lengthy primes in a single column. While this presentation could make the original logic of the covering difficult to follow, it serves to keep white space from over-abounding in the tables.

A.1 Covering systems for $b = 2$

For $b = 2$, our system of congruences results in a modulus M on the order of 10^{19}, or 2^{64}. In Table A.1 we exhibit a covering corresponding to Lemma A.1 (i) which allows a leading 0 in binary to be changed to a 1.

Table A.1 Covering for $A + 1 \cdot 2^k$

row	congruence	prime p_i
1	$k \equiv 0 \pmod{2}$	3
2	$k \equiv 1 \pmod{4}$	5
3	$k \equiv 3 \pmod{8}$	17
4	$k \equiv 7 \pmod{16}$	257
5	$k \equiv 15 \pmod{32}$	65537
6	$k \equiv 31 \pmod{64}$	641
7	$k \equiv 63 \pmod{64}$	6700417

A.2 Covering systems for $b = 3$

For $b = 3$, our system of congruences results in a modulus M on the order of 10^{104}, or 3^{217}. The smallest widely digitally delicate probable prime in base 3 that we have found using such a system is

$$5120877327448131034832807280427377535287031695776660035246304813627518 5-$$

$$67220412643945813184496511521666 53.$$

We take $A \equiv 1 \pmod{2}$ so that $A + 1 \cdot 3^k$ is divisible by 2. Table A.2 exhibits a covering which allows for a leading 0 to be changed to a 2 in base 3.

Table A.2 Covering for $A + 2 \cdot 3^k$

congruence	prime p_i
$k \equiv 0 \pmod 3$	13
$k \equiv 1 \pmod 6$	7
$k \equiv 2 \pmod 9$	757
$k \equiv 8 \pmod{18}$	19
$k \equiv 14 \pmod{18}$	37
$k \equiv 0 \pmod 4$	5
$k \equiv 10 \pmod{12}$	73
$k \equiv 5 \pmod{36}$	530713
$k \equiv 3 \pmod 8$	41

congruence	prime p_i
$k \equiv 17 \pmod{72}$	282429005041
$k \equiv 53 \pmod{144}$	1418632417
$k \equiv 125 \pmod{144}$	56227703611393
$k \equiv 23 \pmod{216}$	2161
$k \equiv 95 \pmod{216}$	15121
$k \equiv 167 \pmod{216}$	10512289
$k \equiv 71 \pmod{108}$	150094634909578633
$k \equiv 143 \pmod{216}$	16569793
$k \equiv 215 \pmod{216}$	3958044610033

A.3 Covering systems for $b = 4$

For $b = 4$, our system of congruences results in a modulus M on the order of 10^{35}, or 4^{58}. We take $A \equiv 2 \pmod 3$ so that $A + 1 \cdot 4^k$ is divisible by 3. Tables A.3 and A.4 exhibit covers which allow for a leading 0 to be changed to a 2 or a 3 in base 4.

Table A.3 Covering for $A + 2 \cdot 4^k$

row	congruence	prime p_i
1	$k \equiv 0 \pmod 2$	5
2	$k \equiv 1 \pmod 4$	17
3	$k \equiv 3 \pmod 8$	257
4	$k \equiv 7 \pmod{16}$	65537
5	$k \equiv 15 \pmod{32}$	641
6	$k \equiv 31 \pmod{32}$	6700417

Table A.4 Covering for $A + 3 \cdot 4^k$

row	congruence	prime p_i
1	$k \equiv 0 \pmod 3$	7
2	$k \equiv 1 \pmod 6$	13
3	$k \equiv 4 \pmod{12}$	241
4	$k \equiv 10 \pmod{24}$	97
5	$k \equiv 22 \pmod{24}$	673
6	$k \equiv 2 \pmod 9$	19
7	$k \equiv 5 \pmod 9$	73
8	$k \equiv 8 \pmod{18}$	37
9	$k \equiv 17 \pmod{18}$	109

A.4 Covering systems for $b = 5$

For $b = 5$, our system of congruences results in a modulus M on the order of 10^{192}, or 5^{275}. We take $A \equiv 1 \pmod 2$ so that $A + 1 \cdot 5^k$ and $A + 3 \cdot 5^k$ are divisible by 2. We exhibit coverings in the tables below corresponding to the other possible digit increases.

Table A.5 Covering for $A + 4 \cdot 5^k$

congruence	prime p_i	congruence	prime p_i
$k \equiv 0 \pmod 5$	11	$k \equiv 23 \pmod{150}$	118801
$k \equiv 1 \pmod 5$	71	$k \equiv 53 \pmod{150}$	20775901
$k \equiv 3 \pmod 6$	7	$k \equiv 83 \pmod{150}$	24665701
$k \equiv 2 \pmod{15}$	181	$k \equiv 113 \pmod{150}$	149439601
$k \equiv 7 \pmod{15}$	1741	$k \equiv 143 \pmod{300}$	14401
$k \equiv 4 \pmod{10}$	521	$k \equiv 293 \pmod{300}$	299541552154912341601
$k \equiv 8 \pmod{20}$	41	$k \equiv 29 \pmod{90}$	60081451169922001
$k \equiv 18 \pmod{20}$	9161	$k \equiv 59 \pmod{180}$	20478961
$k \equiv 12 \pmod{30}$	61	$k \equiv 149 \pmod{180}$	6794091374761
$k \equiv 13 \pmod{30}$	7621	$k \equiv 89 \pmod{180}$	25535754811081
$k \equiv 19 \pmod{60}$	2281	$k \equiv 179 \pmod{360}$	8641
$k \equiv 49 \pmod{60}$	69566521	$k \equiv 359 \pmod{360}$	440641

Table A.6 Covering for $A + 2 \cdot 5^k$

congruence	prime p_i	congruence	prime p_i
$k \equiv 0 \pmod 3$	31	$k \equiv 11 \pmod{24}$	390001
$k \equiv 0 \pmod 2$	3	$k \equiv 23 \pmod{48}$	152587500001
$k \equiv 1 \pmod 6$	7	$k \equiv 47 \pmod{96}$	97
$k \equiv 5 \pmod{12}$	601	$k \equiv 95 \pmod{96}$	240031591394168814433

A.5 Covering systems for $b = 6$

For $b = 6$, our system of congruences results in a modulus M on the order of 10^{483}, or 6^{620}. We take $A \equiv 2 \pmod 5$ so that $A + 3 \cdot 6^k$ is divisible by 5. We exhibit coverings in the tables below corresponding to increasing a digit in base 6 by the other possible increases of 1, 2, 4, or 5.

Table A.7 Covering for $A + 1 \cdot 6^k$

row	congruence	prime p_i
1	$k \equiv 4 \pmod 6$	31
2	$k \equiv 0 \pmod 9$	19
3	$k \equiv 6 \pmod 9$	2467
4	$k \equiv 1 \pmod{12}$	13
5	$k \equiv 7 \pmod{12}$	97
6	$k \equiv 3 \pmod{18}$	46441
7	$k \equiv 12 \pmod{36}$	73
8	$k \equiv 30 \pmod{36}$	541
9	$k \equiv 2 \pmod 3$	43

Table A.8 Covering for $A + 2 \cdot 6^k$

row	congruence	prime p_i
1	$k \equiv 0 \pmod 2$	7
2	$k \equiv 1 \pmod 4$	37
3	$k \equiv 3 \pmod 8$	1297
4	$k \equiv 7 \pmod{16}$	17
5	$k \equiv 15 \pmod{16}$	98801

Table A.9 Covering for $A + 4 \cdot 6^k$

congruence	prime p_i
$0 \pmod 5$	311
$1 \pmod{10}$	11
$6 \pmod{10}$	101
$2 \pmod{15}$	1171
$7 \pmod{15}$	1201
$12 \pmod{45}$	2161
$27 \pmod{45}$	112771
$42 \pmod{45}$	19353635731
$3 \pmod{20}$	241
$8 \pmod{20}$	6781
$13 \pmod{40}$	41
$33 \pmod{40}$	68754507401
$18 \pmod{60}$	61
$38 \pmod{60}$	74161
$58 \pmod{60}$	181
$4 \pmod{25}$	18198701
$9 \pmod{25}$	40185601
$14 \pmod{50}$	3655688315536801
$39 \pmod{100}$	343801
$89 \pmod{100}$	22243201
$19 \pmod{75}$	601
$44 \pmod{75}$	82051
$69 \pmod{75}$	271041511600591342728451
$24 \pmod{125}$	9536585501
$49 \pmod{125}$	117811792772681609501
$74 \pmod{125}$	105875321588567599765751
$99 \pmod{125}$	109844576780875090397325 1
$124 \pmod{250}$	251
$249 \pmod{250}$	751

We use each of the primes 7, 13, and 31 twice over Tables A.7, A.8 and A.10. One checks that our choices are equivalent to $A \equiv 5 \pmod 7$, $A \equiv 7 \pmod{13}$, and $A \equiv 6 \pmod{31}$. For Table A.10 we set

$$p_{11} = 22452257707354557235348829785471057921.$$

Table A.10 Covering for $A + 5 \cdot 6^k$

congruence	prime p_i	congruence	prime p_i
1 (mod 2)	7	54 (mod 108)	591841
2 (mod 6)	31	90 (mod 108)	171467713
4 (mod 12)	13	24 (mod 108)	932461936453
10 (mod 24)	1678321	60 (mod 216)	433
22 (mod 48)	5953	168 (mod 216)	115963921
46 (mod 48)	473896897	96 (mod 216)	8781208996949976153601
0 (mod 36)	55117	204 (mod 216)	241282001155985351966017
6 (mod 72)	577	30 (mod 180)	9001
42 (mod 72)	3313	66 (mod 180)	211501
12 (mod 72)	2478750186961	102 (mod 180)	2106930961
48 (mod 144)	p_{11}	138 (mod 180)	5597780112726834061
120 (mod 288)	115777	174 (mod 540)	4861
264 (mod 288)	31057921	354 (mod 540)	39326041
18 (mod 108)	109	534 (mod 540)	51353541541

A.6 Covering systems for $b = 7$

For $b = 7$, our system of congruences results in a modulus M on the order of 10^{711}, or 7^{841}. We take $A \equiv 1 \pmod 2$ so that $A + 1 \cdot 7^k$, $A + 3 \cdot 7^k$, and $A + 5 \cdot 7^k$ are divisible by 2. We also take $A \equiv 1 \pmod 3$ so that $A + 2 \cdot 7^k$ is divisible by 3. We exhibit coverings below corresponding to the other possible digit increases in base 7.

For Table A.12, we set

$$p_{12} = 217648180992721729506406538251, \quad p_{15} = 2182816753758823696751,$$

$$p_{16} = 590354667835684444020417934211947301188761723956532380043550 1,$$

$$p_{42} = 271796439196451766191391111220539009912588742400633481231401,$$

$$p_{23} = 353207957997402826578121, \quad p_{50} = 11193638545408118035815864041.$$

We obtain the factorization

$$\Phi_{490}(7) = 491 \cdot 12251 \cdot 20632921 \cdot 648128907712931 \cdot p_{50} \cdot C_{490}$$

and again use the notation $p_{n,1}, p_{n,2}$ to refer to two distinct primes dividing C_n.

Table A.11 Covering for $A + 4 \cdot 7^k$

row	congruence	prime p_i
1	$k \equiv 0 \pmod 3$	19
2	$k \equiv 0 \pmod 4$	5
3	$k \equiv 1 \pmod 6$	43
4	$k \equiv 2 \pmod{12}$	13
5	$k \equiv 10 \pmod{12}$	181
6	$k \equiv 5 \pmod{24}$	73
7	$k \equiv 17 \pmod{24}$	193
8	$k \equiv 11 \pmod{24}$	409
9	$k \equiv 23 \pmod{48}$	33232924804801
10	$k \equiv 47 \pmod{96}$	97
11	$k \equiv 95 \pmod{96}$	104837857

Table A.12 Covering for $A + 6 \cdot 7^k$

congruence	prime p_i
0 (mod 5)	2801
1 (mod 10)	11
6 (mod 10)	191
2 (mod 15)	31
7 (mod 15)	159871
12 (mod 30)	6568801
27 (mod 60)	61
3 (mod 25)	2551
38 (mod 100)	101
88 (mod 100)	13001
18 (mod 75)	29251
43 (mod 75)	p_{12}
68 (mod 150)	151
23 (mod 125)	251
48 (mod 125)	p_{15}
73 (mod 125)	p_{16}
98 (mod 250)	751
14 (mod 70)	71
49 (mod 70)	421
59 (mod 210)	211
29 (mod 175)	701
169 (mod 350)	3851
139 (mod 245)	p_{23}
174 (mod 490)	491
419 (mod 490)	12251
57 (mod 60)	555915824341
8 (mod 25)	31280679788951
13 (mod 50)	79787519018560501
143 (mod 150)	6005492312551
223 (mod 250)	1173001
123 (mod 250)	4833574921448501
248 (mod 250)	31818863467130251
4 (mod 35)	2127431041
9 (mod 35)	77192844961
19 (mod 70)	12128131
54 (mod 70)	603926681
24 (mod 140)	102314938321
94 (mod 140)	18690488255321
129 (mod 210)	338640865331157691
199 (mod 210)	450798894542150330401
64 (mod 175)	1237578612719152201
99 (mod 175)	p_{42}
134 (mod 175)	1094471317606762277701
344 (mod 350)	8230203760252601
34 (mod 245)	4896864001
69 (mod 245)	9152363081
104 (mod 245)	11492120512321
209 (mod 490)	20632921
454 (mod 490)	648128907712931
244 (mod 490)	p_{50}
489 (mod 490)	$p_{490,1}$

A.7 Covering systems for $b = 8$

For $b = 8$, our system of congruences results in a modulus M on the order of 10^{1728}, or 8^{1914}. We take $A \equiv 4 \pmod 7$ so that $A + 3 \cdot 8^k$ is divisible by 7. We exhibit coverings in the tables below corresponding to the other possible digit increases in base 8.

We make repeated use of the primes 3, 5, and 17 in Tables A.13, A.14, A.15 and A.16. One checks that our choices are equivalent to $A \equiv 1 \pmod 3$, $A \equiv 4 \pmod 5$, and $A \equiv 4 \pmod{17}$.

Table A.13 Covering for $A + 1 \cdot 8^k$

row	congruence	prime p_i
1	$k \equiv 1 \pmod 2$	3
2	$k \equiv 0 \pmod 4$	5

row	congruence	prime p_i
3	$k \equiv 2 \pmod 8$	17
4	$k \equiv 6 \pmod 8$	241

Table A.14 Covering for $A + 2 \cdot 8^k$

row	congruence	prime p_i
1	$k \equiv 0 \pmod 2$	3
2	$k \equiv 1 \pmod 4$	5
3	$k \equiv 3 \pmod 4$	13

Table A.15 Covering for $A + 4 \cdot 8^k$

row	congruence	prime p_i
1	$k \equiv 1 \pmod 2$	3
2	$k \equiv 2 \pmod 4$	5
3	$k \equiv 4 \pmod 8$	17

row	congruence	prime p_i
4	$k \equiv 0 \pmod{16}$	97
5	$k \equiv 8 \pmod{16}$	257

Table A.16 Covering for $A + 5 \cdot 8^k$

row	congruence	prime p_i
1	$k \equiv 0 \pmod 2$	3
2	$k \equiv 0 \pmod 5$	31
3	$k \equiv 1 \pmod 5$	151
4	$k \equiv 3 \pmod{10}$	11

row	congruence	prime p_i
5	$k \equiv 7 \pmod{10}$	331
6	$k \equiv 9 \pmod{20}$	41
7	$k \equiv 19 \pmod{20}$	61

For Table A.20, we list partial factorizations of $\Phi_n(8)$ in Table A.18.

Table A.17 Covering for $A + 6 \cdot 8^k$

row	congruence	prime p_i
1	$k \equiv 0 \pmod 3$	73
2	$k \equiv 1 \pmod 6$	19
3	$k \equiv 4 \pmod{12}$	37
4	$k \equiv 10 \pmod{12}$	109
5	$k \equiv 2 \pmod 9$	262657
6	$k \equiv 5 \pmod{18}$	87211
7	$k \equiv 14 \pmod{36}$	246241
8	$k \equiv 32 \pmod{36}$	279073
9	$k \equiv 8 \pmod{27}$	2593
10	$k \equiv 17 \pmod{27}$	71119
11	$k \equiv 26 \pmod{27}$	97685839

Table A.18 Partial factorizations of $\Phi_n(8)$ for large n

n	Partial factorization of $\Phi_n(8)$
245	$1471 \cdot 41161 \cdot 4163041 \cdot C_{245}$
343	$6073159 \cdot 1428389887 \cdot C_{343}$
686	$8233 \cdot 2513690593 \cdot C_{686}$
1029	$271657 \cdot C_{1029}$

Table A.19 First part of covering for $A + 7 \cdot 8^k$

row	congruence	prime p_i
1	$k \equiv 0 \pmod 7$	127
2	$k \equiv 1 \pmod 7$	337
3	$k \equiv 2 \pmod{14}$	43
4	$k \equiv 9 \pmod{14}$	5419
5	$k \equiv 3 \pmod{21}$	92737
6	$k \equiv 10 \pmod{21}$	649657
7	$k \equiv 17 \pmod{42}$	77158673929
8	$k \equiv 38 \pmod{84}$	40388473189
9	$k \equiv 80 \pmod{84}$	118750098349
10	$k \equiv 4 \pmod{35}$	71
11	$k \equiv 11 \pmod{35}$	29191
12	$k \equiv 18 \pmod{35}$	106681
13	$k \equiv 25 \pmod{35}$	122921
14	$k \equiv 32 \pmod{35}$	152041
15	$k \equiv 5 \pmod{70}$	211
16	$k \equiv 12 \pmod{70}$	281
17	$k \equiv 19 \pmod{70}$	86171
18	$k \equiv 26 \pmod{70}$	664441

Table A.20 Second part of covering for $A + 7 \cdot 8^k$

row	congruence	prime p_i
19	$k \equiv 33 \pmod{70}$	1564921
20	$k \equiv 40 \pmod{140}$	421
21	$k \equiv 110 \pmod{140}$	7416361
22	$k \equiv 47 \pmod{140}$	146919792181
23	$k \equiv 117 \pmod{140}$	1041815865690181
24	$k \equiv 54 \pmod{210}$	1765891
25	$k \equiv 124 \pmod{210}$	1124770259967650548- 1447137991664348691
26	$k \equiv 194 \pmod{420}$	2521
27	$k \equiv 404 \pmod{420}$	1711081
28	$k \equiv 61 \pmod{350}$	1051
29	$k \equiv 131 \pmod{350}$	110251
30	$k \equiv 201 \pmod{350}$	3205651
31	$k \equiv 271 \pmod{350}$	247772800801
32	$k \equiv 341 \pmod{350}$	347833278451
33	$k \equiv 68 \pmod{350}$	7223591273619001
34	$k \equiv 138 \pmod{350}$	34010032331525251
35	$k \equiv 208 \pmod{350}$	129266711542799251
36	$k \equiv 278 \pmod{350}$	2310141222312973778401
37	$k \equiv 348 \pmod{700}$	701
38	$k \equiv 698 \pmod{700}$	6301
39	$k \equiv 6 \pmod{49}$	4432676798593
40	$k \equiv 13 \pmod{49}$	2741672362528725535068727
41	$k \equiv 20 \pmod{98}$	748819

row	congruence	prime p_i
42	$k \equiv 69 \pmod{98}$	4363953127297
43	$k \equiv 27 \pmod{98}$	26032885845392093851
44	$k \equiv 76 \pmod{196}$	197
45	$k \equiv 174 \pmod{196}$	540961
46	$k \equiv 34 \pmod{196}$	19707683773
47	$k \equiv 83 \pmod{196}$	4981857697937
48	$k \equiv 132 \pmod{196}$	40544859693521152369
49	$k \equiv 181 \pmod{196}$	17059410504738323992180849
50	$k \equiv 41 \pmod{245}$	1471
51	$k \equiv 90 \pmod{245}$	41161
52	$k \equiv 139 \pmod{245}$	4163041
53	$k \equiv 188 \pmod{245}$	$p_{245,1}$
54	$k \equiv 237 \pmod{245}$	$p_{245,2}$
55	$k \equiv 48 \pmod{343}$	6073159
56	$k \equiv 97 \pmod{343}$	1428389887
57	$k \equiv 146 \pmod{343}$	$p_{343,1}$
58	$k \equiv 195 \pmod{343}$	$p_{343,2}$
59	$k \equiv 244 \pmod{686}$	8233
60	$k \equiv 587 \pmod{686}$	2513690593
61	$k \equiv 293 \pmod{686}$	$p_{686,1}$
62	$k \equiv 636 \pmod{686}$	$p_{686,2}$
63	$k \equiv 342 \pmod{1029}$	271657
64	$k \equiv 685 \pmod{1029}$	$p_{1029,1}$
65	$k \equiv 1028 \pmod{1029}$	$p_{1029,2}$

A.8 Covering systems for $b = 9$

For $b = 9$, our system of congruences results in a modulus M on the order of 10^{179}, or 9^{188}. We take $A \equiv 1 \pmod 2$ so that $A + (2j+1) \cdot 9^k$ is divisible by 2. We exhibit coverings below corresponding to increasing a digit in base 9 by an even amount.

Table A.21 Covering for $A + 6 \cdot 9^k$

row	congruence	prime p_i
1	$k \equiv 0 \pmod 3$	7
2	$k \equiv 1 \pmod 3$	13
3	$k \equiv 2 \pmod 6$	73
4	$k \equiv 5 \pmod{12}$	6481
5	$k \equiv 11 \pmod{24}$	97
6	$k \equiv 23 \pmod{24}$	577

We use each of the primes 5 and 17 twice over Tables A.22, A.23, and A.24. One checks that our choices are equivalent to $A \equiv 3 \pmod 5$ and $A \equiv 4 \pmod{17}$.

Table A.22 Covering for $A + 2 \cdot 9^k$

row	congruence	prime p_i
1	$k \equiv 0 \pmod 2$	5
2	$k \equiv 1 \pmod 4$	41
3	$k \equiv 3 \pmod 8$	17
4	$k \equiv 7 \pmod 8$	193

Table A.23 Covering for $A + 4 \cdot 9^k$

row	congruence	prime p_i
1	$k \equiv 4 \pmod 8$	17
2	$k \equiv 0 \pmod 5$	11
3	$k \equiv 1 \pmod 5$	61
4	$k \equiv 3 \pmod{10}$	1181
5	$k \equiv 18 \pmod{20}$	42521761
6	$k \equiv 8 \pmod{40}$	14401
7	$k \equiv 2 \pmod{15}$	31
8	$k \equiv 7 \pmod{15}$	271

row	congruence	prime p_i
9	$k \equiv 12 \pmod{15}$	4561
10	$k \equiv 4 \pmod{25}$	151
11	$k \equiv 9 \pmod{25}$	8951
12	$k \equiv 14 \pmod{25}$	391151
13	$k \equiv 19 \pmod{25}$	22996651
14	$k \equiv 24 \pmod{50}$	101
15	$k \equiv 49 \pmod{50}$	394201

Table A.24 Covering for $A + 8 \cdot 9^k$

row	congruence	prime p_i
1	$k \equiv 1 \pmod 2$	5
2	$k \equiv 0 \pmod 7$	547
3	$k \equiv 1 \pmod 7$	1093
4	$k \equiv 2 \pmod{14}$	29
5	$k \equiv 4 \pmod{14}$	16493
6	$k \equiv 6 \pmod{28}$	430697
7	$k \equiv 20 \pmod{28}$	647753
8	$k \equiv 10 \pmod{42}$	2857
9	$k \equiv 24 \pmod{42}$	109688713
10	$k \equiv 38 \pmod{84}$	337
11	$k \equiv 80 \pmod{84}$	673
12	$k \equiv 12 \pmod{70}$	28596961
13	$k \equiv 26 \pmod{70}$	32839661
14	$k \equiv 40 \pmod{70}$	94373861
15	$k \equiv 54 \pmod{140}$	281
16	$k \equiv 124 \pmod{140}$	18481
17	$k \equiv 68 \pmod{140}$	369879560116990841
18	$k \equiv 138 \pmod{140}$	3353336738929580410561

A.9 Covering systems for $b = 11$

For $b = 11$, our system of congruences results in a modulus M on the order of 10^{365}, or 11^{351}. We take $A \equiv 1 \pmod 2$ so that $A + (2j+1) \cdot 11^k$ is divisible by 2. We also take $A \equiv 3 \pmod 5$ so that $A + 2 \cdot 11^k$ is divisible by 5. We exhibit coverings below corresponding to increasing a digit in base 11 by other possible amounts. The prime 3 is used multiple times and in each case corresponds to $A \equiv 2 \pmod 3$.

Table A.25 Covering for $A + 4 \cdot 11^k$

row	congruence	prime p_i
1	$k \equiv 0 \pmod 2$	3
2	$k \equiv 1 \pmod 4$	61
3	$k \equiv 3 \pmod 8$	7321
4	$k \equiv 7 \pmod{16}$	17
5	$k \equiv 15 \pmod{16}$	6304673

Table A.26 Covering for $A + 10 \cdot 11^k$

congruence	prime p_i
0 (mod 2)	3
0 (mod 7)	43
1 (mod 7)	45319
3 (mod 14)	1623931
5 (mod 28)	29
19 (mod 28)	1933
9 (mod 28)	55527473
23 (mod 56)	113
51 (mod 56)	449
11 (mod 56)	2521

congruence	prime p_i
25 (mod 56)	77001139434480073
39 (mod 112)	337
95 (mod 112)	394129
53 (mod 112)	236352238647181441
109 (mod 112)	30904439623835951233791 37
13 (mod 42)	3421169496361
27 (mod 84)	19069
69 (mod 84)	520799717831587692709
41 (mod 126)	3304981
83 (mod 126)	468843103
125 (mod 126)	71596275661

Table A.27 Covering for $A + 8 \cdot 11^k$

congruence	prime p_i
1 (mod 2)	3
0 (mod 5)	3221
2 (mod 10)	13421
4 (mod 20)	212601841
14 (mod 40)	41
6 (mod 30)	31
16 (mod 30)	7537711
26 (mod 90)	181
56 (mod 90)	631
8 (mod 50)	46601
28 (mod 100)	101

congruence	prime p_i
34 (mod 40)	1120648576818041
86 (mod 90)	86306335830799838011
18 (mod 50)	14436295738510501
78 (mod 100)	2248313994601
38 (mod 100)	19930999065427108197278845 01
88 (mod 200)	401
188 (mod 200)	2254601
48 (mod 150)	751
98 (mod 150)	299401
148 (mod 150)	20128755258227254- 47651340174136551

Table A.28 Covering for $A + 6 \cdot 11^k$

row	congruence	prime p_i
1	$k \equiv 0 \pmod 3$	7
2	$k \equiv 1 \pmod 3$	19
3	$k \equiv 2 \pmod 6$	37

row	congruence	prime p_i
4	$k \equiv 4 \pmod{12}$	13
5	$k \equiv 10 \pmod{12}$	1117

A.10 Covering systems for $b = 31$

For $b = 31$, we did not determine the size of the modulus M resulting from our system of congruences. We take $A \equiv 1 \pmod 2$ so that $A+(2j+1)\cdot 31^k$ is divisible by 2. We

also take $A \equiv 2 \pmod 3$ so that $A+(3j+1)\cdot 31^k$ is divisible by 3, and we furthermore set $A \equiv 1 \pmod 5$ so that $A + (5j + 4) \cdot 31^k$ is divisible by 5. We exhibit coverings below corresponding to increasing a digit in base 31 by other possible amounts. The primes 7, 11, 13, 17, 19, 37 are used multiple times below and each use corresponds to one of the following congruences.

$$A \equiv 5 \pmod 7, \quad A \equiv 5 \pmod{11}, \quad A \equiv 5 \pmod{13},$$

$$A \equiv 12 \pmod{17}, \quad A \equiv 11 \pmod{19}, \quad A \equiv 11 \pmod{37}.$$

Table A.29 Covering for $A + 26 \cdot 31^k$

row	congruence	prime p_i
1	$k \equiv 3 \pmod 6$	7
2	$k \equiv 1 \pmod 6$	19
3	$k \equiv 0 \pmod 4$	37
4	$k \equiv 11 \pmod{16}$	17
5	$k \equiv 5 \pmod{18}$	577
6	$k \equiv 11 \pmod{18}$	1538083
7	$k \equiv 17 \pmod{36}$	1536553
8	$k \equiv 35 \pmod{36}$	512616735577
9	$k \equiv 2 \pmod{12}$	922561
10	$k \equiv 6 \pmod{24}$	852890113921
11	$k \equiv 22 \pmod{72}$	73
12	$k \equiv 46 \pmod{72}$	4683817
13	$k \equiv 70 \pmod{72}$	1814503763676130449408979921
14	$k \equiv 18 \pmod{120}$	35401
15	$k \equiv 42 \pmod{120}$	1546081
16	$k \equiv 66 \pmod{120}$	966778313342560511941015599854119260 1
17	$k \equiv 90 \pmod{240}$	241
18	$k \equiv 210 \pmod{240}$	32360641
19	$k \equiv 114 \pmod{240}$	362634922081
20	$k \equiv 234 \pmod{240}$	69916284426778163281
20	$k \equiv 10 \pmod{48}$	97
20	$k \equiv 34 \pmod{48}$	7499207440683838894753

For the tables that follow, we list partial factorizations of $\Phi_n(31)$ in Table A.31 and Table A.32. In addition to the values displayed there, we use the notation

$$\Phi_{176}(31) = P_{176} \quad \text{and} \quad \Phi_{420}(31) = P_{420}$$

Table A.30 Covering for $A + 30 \cdot 31^k$

row	congruence	prime p_i
1	$k \equiv 1 \pmod 3$	331
2	$k \equiv 0 \pmod 6$	7
3	$k \equiv 3 \pmod 6$	19
4	$k \equiv 2 \pmod 9$	3637
5	$k \equiv 5 \pmod 9$	81343
6	$k \equiv 8 \pmod{27}$	1836205027201
7	$k \equiv 17 \pmod{27}$	126901881805771
8	$k \equiv 26 \pmod{81}$	2593
9	$k \equiv 53 \pmod{81}$	13933
10	$k \equiv 80 \pmod{81}$	477739

for values which were determined to be prime. We also use

$$\Phi_{208}(31) = C_{208}, \quad \Phi_{325}(31) = C_{325}, \quad \Phi_{425}(31) = C_{425}, \quad \Phi_{520}(31) = C_{520},$$

$$\Phi_{588}(31) = C_{588}, \quad \Phi_{1275}(31) = C_{1275}, \quad \Phi_{1530}(31) = C_{1530}, \quad \text{and} \quad \Phi_{1540}(31) = C_{1540}$$

for values which we determined to have at least 2 prime factors but for which we could not find any prime divisors. Table A.33 displays complete factorizations with notation used for primes where were too lengthy to display.

For Tables A.35 and A.36 we set

$$p_{21} = 272620054274111996657517726155748513108418866372275455497228 1,$$

$$p_{31} = 660479435423419861325502790686400761533380000744579973299352935629 -$$

$$42426481, \quad p_{86} = 22472120241291866633457681925052319136 9,$$

$$p_{39} = 348673230951446260771883379412341320615347347601103310801195979086 -$$

$$277, \quad p_{83} = 11293636368958098920863036926271138717 21,$$

$$p_{68} = 29510535204545262157687088665468191183896988343413667225871.$$

Table A.31 Partial factorizations of $\Phi_n(31)$ for large n

n	Partial factorization of $\Phi_n(31)$
91	$2549 \cdot 1661479 \cdot C_{91}$
117	$2534689 \cdot C_{117}$
125	$251 \cdot 129001 \cdot 12181751 \cdot C_{125}$
135	$1344742561 \cdot C_{135}$
147	$883 \cdot C_{147}$
160	$380641 \cdot 1176641 \cdot 8084410241 \cdot C_{160}$
195	$35956831 \cdot C_{195}$
238	$11781795397 \cdot 2744226674742050863 \cdot C_{238}$
245	$491 \cdot 55848731 \cdot C_{245}$
255	$934831 \cdot C_{255}$
264	$183516169 \cdot C_{264}$
306	$307 \cdot 78198146102753533 \cdot 19220209997787857 \cdot C_{306}$
320	$259201 \cdot 59826881 \cdot C_{320}$
330	$2995081 \cdot C_{330}$
340	$1361 \cdot 3061 \cdot 30941 \cdot 2964461 \cdot 5153381 \cdot C_{340}$
351	$132679 \cdot 445069 \cdot 175071781 \cdot 1467780211 \cdot C_{351}$
352	$353 \cdot C_{352}$
357	$637603 \cdot 2112727 \cdot C_{357}$
385	$2311 \cdot C_{385}$
390	$188431581362701 \cdot 9708046814116951 \cdot C_{390}$
392	$29401 \cdot 946681 \cdot C_{392}$
416	$1404631073 \cdot C_{416}$
455	$6041004971 \cdot C_{455}$
459	$1131567193 \cdot C_{459}$

n	Partial factorization of $\Phi_n(31)$
468	$937 \cdot 1015561 \cdot C_{468}$
480	$20641 \cdot 330991018976905188481 \cdot C_{480}$
490	$1471 \cdot 32341 \cdot 10996091 \cdot C_{490}$
595	$89278561 \cdot 108837401 \cdot 42498121331$ $\cdot 393384880321890060440004 1 \cdot C_{595}$
612	$15913 \cdot 34273 \cdot C_{612}$
650	$391301 \cdot 45514951 \cdot 1431069251 \cdot$
680	$3576121 \cdot C_{680}$
765	$1531 \cdot 6121 \cdot 1074061 \cdot 8197741 \cdot C_{765}$
770	$2868251 \cdot C_{770}$
780	$17329261 \cdot 45796141 \cdot C_{780}$
850	$40801 \cdot C_{850}$
882	$154351 \cdot C_{882}$
910	$131041 \cdot C_{910}$
1040	$2081 \cdot 2057345681 \cdot C_{1040}$
1071	$39307843 \cdot C_{1071}$
1190	$2381 \cdot C_{1190}$
1224	$29841121 \cdot 209530441 \cdot 330188689$ $\cdot 1133681368703716513$ $\cdot 61410533730626180017 \cdot C_{1224}$
1248	$4993 \cdot 2215201 \cdot C_{1248}$
1300	$4479139601 \cdot C_{1300}$
1365	$2731 \cdot 2435161 \cdot C_{1365}$
1470	$282506071 \cdot C_{1470}$

Table A.32 More partial factorizations of $\Phi_n(31)$ for large n

n	Factorization of $\Phi_n(31)$
1560	$41461681 \cdot C_{1560}$
1820	$14990810381 \cdot C_{1820}$
1872	$282419281 \cdot C_{1872}$
2142	$53551 \cdot 8281014336631 \cdot 17562188355029137 \cdot C_{2142}$
2275	$50051 \cdot 54601 \cdot C_{2275}$
2448	$637045489 \cdot C_{2448}$
2295	$4591 \cdot 9181 \cdot 59671 \cdot C_{2295}$
2550	$2551 \cdot C_{2550}$
3213	$7812268926269851 \cdot C_{3213}$
3744	$5814433 \cdot C_{3744}$
4284	$5714857 \cdot C_{4284}$
4590	$2519911 \cdot C_{4590}$

Table A.33 Complete factorizations of $\Phi_n(31)$ for large n

n	Factorization of $\Phi_n(31)$
64	$4801 \cdot P_{64}$
85	$108971 \cdot 391206807721 \cdot 21736504684553261 \cdot P_{85}$
119	$239 \cdot 2857 \cdot 78541 \cdot P_{119}$
153	$17137 \cdot 42834601810502407 \cdot P_{153}$
165	$1321 \cdot P_{165}$
170	$232122807601 \cdot P_{170}$
180	$8728381 \cdot 14398921 \cdot P_{180}$
196	$197 \cdot P_{196}$
200	$601 \cdot 7137001 \cdot P_{200}$
260	$1301 \cdot 22765081 \cdot P_{260}$
312	$313 \cdot 4292809 \cdot 135272593 \cdot 115436220433 \cdot P_{312}$
936	$7489 \cdot P_{936}$

Table A.34 Covering for $A + 8 \cdot 31^k$

row	congruence	prime p_i
1	$k \equiv 2 \pmod 6$	7
2	$k \equiv 0 \pmod 6$	19
3	$k \equiv 0 \pmod 4$	13
4	$k \equiv 1 \pmod 4$	37
5	$k \equiv 2 \pmod 8$	409
6	$k \equiv 6 \pmod 8$	1129

row	congruence	prime p_i
7	$k \equiv 3 \pmod{16}$	17
8	$k \equiv 7 \pmod{16}$	25085030513
9	$k \equiv 11 \pmod{32}$	1889
10	$k \equiv 27 \pmod{32}$	1347329
11	$k \equiv 15 \pmod{32}$	6139297
12	$k \equiv 31 \pmod{32}$	23277313

Table A.35 First part of covering for $A + 2 \cdot 31^k$

row	congruence	prime p_i
1	$k \equiv 0 \pmod 6$	7
2	$k \equiv 15 \pmod{16}$	17
3	$k \equiv 3 \pmod 5$	11
4	$k \equiv 0 \pmod{13}$	42407
5	$k \equiv 1 \pmod{13}$	2426789
6	$k \equiv 2 \pmod{13}$	7908811
7	$k \equiv 3 \pmod{26}$	17863
8	$k \equiv 16 \pmod{26}$	42716694944587
9	$k \equiv 4 \pmod{39}$	79
10	$k \equiv 17 \pmod{39}$	13807
11	$k \equiv 30 \pmod{39}$	39703
12	$k \equiv 5 \pmod{52}$	53
13	$k \equiv 18 \pmod{52}$	116337521
14	$k \equiv 31 \pmod{52}$	76037563733
15	$k \equiv 44 \pmod{52}$	101686136508893
16	$k \equiv 6 \pmod{39}$	175500339130677572941801
17	$k \equiv 19 \pmod{78}$	157
18	$k \equiv 58 \pmod{78}$	238213
19	$k \equiv 32 \pmod{78}$	171233702673319174255441807 21
20	$k \equiv 71 \pmod{156}$	141336778441
21	$k \equiv 149 \pmod{156}$	p_{21}
22	$k \equiv 7 \pmod{91}$	2549
23	$k \equiv 20 \pmod{91}$	1661479

row	congruence	prime p_i
24	$k \equiv 33 \pmod{91}$	$p_{91,1}$
25	$k \equiv 46 \pmod{91}$	$p_{91,2}$
26	$k \equiv 59 \pmod{182}$	547
27	$k \equiv 150 \pmod{182}$	1093
28	$k \equiv 72 \pmod{182}$	647001
29	$k \equiv 163 \pmod{182}$	14407667
30	$k \equiv 85 \pmod{182}$	669665808855863
31	$k \equiv 176 \pmod{182}$	p_{31}
32	$k \equiv 8 \pmod{117}$	2534689
33	$k \equiv 21 \pmod{117}$	$p_{117,1}$
34	$k \equiv 34 \pmod{117}$	$p_{117,2}$
35	$k \equiv 47 \pmod{234}$	4447
36	$k \equiv 164 \pmod{234}$	7776289
37	$k \equiv 60 \pmod{234}$	21931507729
38	$k \equiv 177 \pmod{234}$	903087677909176579
39	$k \equiv 73 \pmod{234}$	p_{39}
40	$k \equiv 190 \pmod{468}$	937
41	$k \equiv 424 \pmod{468}$	1015561
42	$k \equiv 86 \pmod{468}$	$p_{468,1}$
43	$k \equiv 203 \pmod{468}$	$p_{468,2}$
44	$k \equiv 320 \pmod{936}$	7489
45	$k \equiv 788 \pmod{936}$	P_{936}
46	$k \equiv 437 \pmod{1872}$	282419281

Table A.36 Second part of covering for $A + 2 \cdot 31^k$

row	congruence	prime p_i
47	$k \equiv 905 \pmod{1872}$	$p_{1872,1}$
48	$k \equiv 1373 \pmod{1872}$	$p_{1872,2}$
49	$k \equiv 1841 \pmod{3744}$	5814433
50	$k \equiv 3713 \pmod{3744}$	$p_{3744,1}$
51	$k \equiv 99 \pmod{351}$	132679
52	$k \equiv 216 \pmod{351}$	445069
53	$k \equiv 333 \pmod{351}$	175071781
54	$k \equiv 112 \pmod{351}$	1467780211
55	$k \equiv 229 \pmod{351}$	$p_{351,1}$
56	$k \equiv 346 \pmod{351}$	$p_{351,2}$
57	$k \equiv 10 \pmod{65}$	911
58	$k \equiv 36 \pmod{195}$	35956831
59	$k \equiv 101 \pmod{195}$	$p_{195,1}$
60	$k \equiv 166 \pmod{195}$	$p_{195,2}$
61	$k \equiv 49 \pmod{260}$	1301
62	$k \equiv 114 \pmod{260}$	22765081
63	$k \equiv 179 \pmod{260}$	P_{260}
64	$k \equiv 244 \pmod{780}$	17329261
65	$k \equiv 504 \pmod{780}$	45796141
66	$k \equiv 764 \pmod{780}$	$p_{780,1}$
67	$k \equiv 62 \pmod{130}$	197271101
68	$k \equiv 127 \pmod{130}$	p_{68}

row	congruence	prime p_i
69	$k \equiv 11 \pmod{65}$	1951
70	$k \equiv 24 \pmod{65}$	5979236519649901
71	$k \equiv 37 \pmod{130}$	131
72	$k \equiv 102 \pmod{130}$	521
73	$k \equiv 50 \pmod{325}$	$p_{325,1}$
74	$k \equiv 115 \pmod{325}$	$p_{325,2}$
75	$k \equiv 180 \pmod{650}$	391301
76	$k \equiv 505 \pmod{650}$	45514951
77	$k \equiv 245 \pmod{650}$	1431069251
78	$k \equiv 570 \pmod{650}$	$p_{650,1}$
79	$k \equiv 310 \pmod{650}$	$p_{650,2}$
80	$k \equiv 635 \pmod{1300}$	4479139601
81	$k \equiv 1285 \pmod{1300}$	$p_{1300,1}$
82	$k \equiv 12 \pmod{65}$	31035996941
83	$k \equiv 25 \pmod{65}$	p_{83}
84	$k \equiv 9 \pmod{104}$	305688893141113
85	$k \equiv 22 \pmod{104}$	5603212901768856193
86	$k \equiv 35 \pmod{104}$	p_{86}
87	$k \equiv 48 \pmod{208}$	$p_{208,1}$
88	$k \equiv 152 \pmod{208}$	$p_{208,2}$
89	$k \equiv 61 \pmod{312}$	313
90	$k \equiv 165 \pmod{312}$	4292809

Table A.37 Third part of covering for $A + 2 \cdot 31^k$

row	congruence	prime p_i
91	$k \equiv 269 \pmod{312}$	135272593
92	$k \equiv 74 \pmod{312}$	115436220433
93	$k \equiv 178 \pmod{312}$	P_{312}
94	$k \equiv 282 \pmod{624}$	1249
95	$k \equiv 594 \pmod{624}$	1873
96	$k \equiv 87 \pmod{416}$	1404631073
97	$k \equiv 191 \pmod{416}$	$p_{416,1}$
98	$k \equiv 295 \pmod{416}$	$p_{416,2}$
99	$k \equiv 399 \pmod{1248}$	4993
100	$k \equiv 815 \pmod{1248}$	2215201
101	$k \equiv 1231 \pmod{1248}$	$p_{1248,1}$
102	$k \equiv 100 \pmod{520}$	$p_{520,1}$
103	$k \equiv 204 \pmod{520}$	$p_{520,2}$
104	$k \equiv 308 \pmod{1040}$	2081
105	$k \equiv 828 \pmod{1040}$	2057345681
106	$k \equiv 412 \pmod{1040}$	$p_{1040,1}$
107	$k \equiv 932 \pmod{1040}$	$p_{1040,2}$
108	$k \equiv 516 \pmod{1560}$	41461681
109	$k \equiv 1036 \pmod{1560}$	$p_{1560,1}$
110	$k \equiv 1556 \pmod{1560}$	$p_{1560,2}$
111	$k \equiv 51 \pmod{455}$	6041004971
112	$k \equiv 116 \pmod{455}$	$p_{455,1}$

row	congruence	prime p_i
113	$k \equiv 181 \pmod{455}$	$p_{455,2}$
114	$k \equiv 246 \pmod{910}$	131041
115	$k \equiv 701 \pmod{910}$	$p_{910,1}$
116	$k \equiv 311 \pmod{1365}$	2731
117	$k \equiv 766 \pmod{1365}$	2435161
118	$k \equiv 1221 \pmod{1365}$	$p_{1365,1}$
119	$k \equiv 376 \pmod{910}$	$p_{910,2}$
120	$k \equiv 831 \pmod{1820}$	14990810381
121	$k \equiv 1741 \pmod{1820}$	$p_{1820,1}$
122	$k \equiv 441 \pmod{2275}$	50051
123	$k \equiv 896 \pmod{2275}$	54601
124	$k \equiv 1351 \pmod{2275}$	$p_{2275,1}$
125	$k \equiv 1806 \pmod{2275}$	$p_{2275,2}$
126	$k \equiv 2261 \pmod{4550}$	22751
127	$k \equiv 4536 \pmod{4550}$	4770770551
128	$k \equiv 64 \pmod{390}$	188431581362701
129	$k \equiv 129 \pmod{390}$	9708046814116951
130	$k \equiv 194 \pmod{390}$	$p_{390,1}$
131	$k \equiv 259 \pmod{390}$	$p_{390,2}$
132	$k \equiv 389 \pmod{1170}$	2341
133	$k \equiv 779 \pmod{1170}$	24571
134	$k \equiv 1169 \pmod{1170}$	111127771

For Table A.38 we set

$$p_{11} = 2818878916995763094949317586889621110823118869067525200 01.$$

Table A.38 Covering for $A + 6 \cdot 31^k$

congruence	prime p_i
0 (mod 5)	11
1 (mod 5)	17351
2 (mod 10)	41
7 (mod 10)	21821
3 (mod 20)	181
13 (mod 20)	4707206941
8 (mod 50)	1901
18 (mod 50)	4726301
28 (mod 50)	74770514303869505101
38 (mod 100)	1601
48 (mod 100)	p_{11}
88 (mod 200)	601
188 (mod 200)	7137001

congruence	prime p_i
98 (mod 200)	P_{200}
198 (mod 400)	401
398 (mod 400)	16001
4 (mod 25)	101
9 (mod 25)	4951
14 (mod 25)	13277801
19 (mod 25)	20235942281002951
24 (mod 125)	251
49 (mod 125)	129001
74 (mod 125)	12181751
99 (mod 125)	$p_{125,1}$
124 (mod 125)	$p_{125,2}$

For Table A.39, we set

$$p_{21} = 23666169664227515305698014619167477661638036769364 1,$$

$$p_{25} = 24106981477091678423113880081946849059226586740161,$$

$$p_{33} = 26376816099614419212000453294285502148676052955945811649400 1319,$$

$$p_{35} = 38220996250661471852777449353929602800708759586204509824640297561 6-$$

$$281748634348102379.$$

For Tables A.42 and A.44, we set

$$p_{12} = 26111666369716154235191813357344284930 7,$$

$$p_{115} = 3933848803218900604400041,$$

$$p_{129} = 38894363106867279162284931624923616 01.$$

Table A.39 First part of covering for $A + 12 \cdot 31^k$

row	congruence	prime p_i
1	$k \equiv 3 \pmod 6$	7
2	$k \equiv 4 \pmod 6$	19
3	$k \equiv 1 \pmod 4$	13
4	$k \equiv 8 \pmod{16}$	17
5	$k \equiv 0 \pmod{11}$	23
6	$k \equiv 1 \pmod{11}$	397
7	$k \equiv 2 \pmod{11}$	617
8	$k \equiv 3 \pmod{11}$	150332843
9	$k \equiv 4 \pmod{22}$	757241
10	$k \equiv 15 \pmod{22}$	1048563011
11	$k \equiv 8 \pmod{33}$	650141690025315305584300036801
12	$k \equiv 5 \pmod{44}$	2729
13	$k \equiv 16 \pmod{44}$	245911396799577828131028569
14	$k \equiv 27 \pmod{88}$	89
15	$k \equiv 71 \pmod{88}$	414407390867564627396249
16	$k \equiv 38 \pmod{88}$	122362906452015011697495593500250 41
17	$k \equiv 82 \pmod{176}$	P_{176}
18	$k \equiv 170 \pmod{352}$	353
19	$k \equiv 346 \pmod{352}$	$p_{352,1}$
20	$k \equiv 6 \pmod{55}$	167767051
21	$k \equiv 17 \pmod{55}$	p_{21}
22	$k \equiv 28 \pmod{110}$	661
23	$k \equiv 83 \pmod{110}$	2531
24	$k \equiv 39 \pmod{110}$	11551
25	$k \equiv 94 \pmod{110}$	p_{25}
26	$k \equiv 50 \pmod{165}$	1321
27	$k \equiv 105 \pmod{165}$	P_{165}
28	$k \equiv 160 \pmod{330}$	2995081
29	$k \equiv 325 \pmod{330}$	$p_{330,1}$
30	$k \equiv 7 \pmod{77}$	2927
31	$k \equiv 18 \pmod{77}$	23503054499
32	$k \equiv 29 \pmod{77}$	16169321243923
33	$k \equiv 40 \pmod{77}$	p_{33}
34	$k \equiv 51 \pmod{154}$	818819
35	$k \equiv 128 \pmod{154}$	p_{35}
36	$k \equiv 62 \pmod{231}$	463
37	$k \equiv 139 \pmod{231}$	13780537
38	$k \equiv 216 \pmod{231}$	816786763717

Table A.40 Second part of covering for $A + 12 \cdot 31^k$

row	congruence	prime p_i
39	$k \equiv 73 \pmod{385}$	2311
40	$k \equiv 150 \pmod{385}$	$p_{385,1}$
41	$k \equiv 227 \pmod{385}$	$p_{385,1}$
42	$k \equiv 304 \pmod{770}$	2868251
43	$k \equiv 689 \pmod{770}$	$p_{770,1}$
44	$k \equiv 381 \pmod{770}$	$p_{770,2}$
45	$k \equiv 766 \pmod{1540}$	$p_{1540,2}$
46	$k \equiv 1536 \pmod{1540}$	$p_{1540,2}$
47	$k \equiv 20 \pmod{99}$	199
48	$k \equiv 53 \pmod{99}$	991
49	$k \equiv 86 \pmod{99}$	204733
50	$k \equiv 32 \pmod{99}$	36093579787
51	$k \equiv 65 \pmod{99}$	294573316951
52	$k \equiv 98 \pmod{99}$	215792743120601131
53	$k \equiv 19 \pmod{99}$	3763784187326467459
54	$k \equiv 52 \pmod{99}$	8695359830927455963 21
55	$k \equiv 85 \pmod{198}$	8713
56	$k \equiv 184 \pmod{198}$	430057
57	$k \equiv 31 \pmod{66}$	67
58	$k \equiv 42 \pmod{66}$	297991
59	$k \equiv 43 \pmod{66}$	34731987261785578083133
60	$k \equiv 54 \pmod{132}$	599382278617
61	$k \equiv 120 \pmod{132}$	169301958609793153
62	$k \equiv 30 \pmod{132}$	44519836064216868275802052842 01
63	$k \equiv 96 \pmod{264}$	183516169
64	$k \equiv 228 \pmod{264}$	$p_{264,1}$

Table A.41 First part of covering for $A + 18 \cdot 31^k$

row	congruence	prime p_i
1	$k \equiv 4 \pmod{6}$	7
2	$k \equiv 2 \pmod{6}$	19
3	$k \equiv 2 \pmod{4}$	13
4	$k \equiv 0 \pmod{15}$	2521
5	$k \equiv 5 \pmod{15}$	327412201
6	$k \equiv 10 \pmod{45}$	271
7	$k \equiv 25 \pmod{45}$	63901
8	$k \equiv 40 \pmod{45}$	106291
9	$k \equiv 1 \pmod{17}$	751670559138758105956097

Table A.42 Second part of covering for $A + 18 \cdot 31^k$

row	congruence	prime p_i
10	$k \equiv 6 \pmod{34}$	103
11	$k \equiv 23 \pmod{34}$	6841661642646463343047
12	$k \equiv 11 \pmod{51}$	p_{12}
13	$k \equiv 28 \pmod{51}$	1961163283
14	$k \equiv 45 \pmod{102}$	2796214962413636917873
15	$k \equiv 96 \pmod{102}$	19533377987335897390783809 7
16	$k \equiv 16 \pmod{68}$	1399577
17	$k \equiv 33 \pmod{68}$	224499664484159761
18	$k \equiv 50 \pmod{68}$	1682325489672499143634073
19	$k \equiv 67 \pmod{136}$	137
20	$k \equiv 135 \pmod{136}$	953
21	$k \equiv 4 \pmod{119}$	239
22	$k \equiv 21 \pmod{119}$	2857
23	$k \equiv 38 \pmod{119}$	78541
24	$k \equiv 55 \pmod{119}$	P_{119}
25	$k \equiv 72 \pmod{238}$	11781795397
26	$k \equiv 191 \pmod{238}$	2744226674742050863
27	$k \equiv 89 \pmod{238}$	$p_{238,1}$
28	$k \equiv 208 \pmod{238}$	$p_{238,2}$
29	$k \equiv 106 \pmod{357}$	637603
30	$k \equiv 225 \pmod{357}$	2112727
31	$k \equiv 344 \pmod{357}$	$p_{357,1}$
32	$k \equiv 9 \pmod{153}$	17137
33	$k \equiv 26 \pmod{153}$	42834601810502407
34	$k \equiv 43 \pmod{153}$	P_{153}

row	congruence	prime p_i
35	$k \equiv 60 \pmod{306}$	307
36	$k \equiv 213 \pmod{306}$	78198146102753533
37	$k \equiv 77 \pmod{306}$	19220209997787857
38	$k \equiv 230 \pmod{306}$	$p_{306,1}$
39	$k \equiv 94 \pmod{459}$	1131567193
40	$k \equiv 247 \pmod{459}$	$p_{459,1}$
41	$k \equiv 400 \pmod{459}$	$p_{459,2}$
42	$k \equiv 111 \pmod{612}$	15913
43	$k \equiv 264 \pmod{612}$	34273
44	$k \equiv 417 \pmod{612}$	$p_{612,1}$
45	$k \equiv 570 \pmod{612}$	$p_{612,2}$
46	$k \equiv 128 \pmod{1224}$	29841121
47	$k \equiv 281 \pmod{1224}$	209530441
48	$k \equiv 434 \pmod{1224}$	330188689
49	$k \equiv 587 \pmod{1224}$	1133681368703716513
50	$k \equiv 740 \pmod{1224}$	61410533730626180017
51	$k \equiv 893 \pmod{1224}$	$p_{1224,1}$
52	$k \equiv 1046 \pmod{1224}$	$p_{1224,2}$
53	$k \equiv 1199 \pmod{2448}$	637045489
54	$k \equiv 2423 \pmod{2448}$	$p_{2448,1}$
55	$k \equiv 145 \pmod{1071}$	39307843
56	$k \equiv 298 \pmod{1071}$	$p_{1071,1}$
57	$k \equiv 451 \pmod{1071}$	$p_{1071,2}$
58	$k \equiv 604 \pmod{2142}$	53551
59	$k \equiv 1675 \pmod{2142}$	8281014336631

Table A.43 Third part of covering for $A + 18 \cdot 31^k$

row	congruence	prime p_i
60	$k \equiv 757 \pmod{2142}$	17562188355029137
61	$k \equiv 1828 \pmod{2142}$	$p_{2142,1}$
62	$k \equiv 910 \pmod{2142}$	$p_{2142,2}$
63	$k \equiv 1981 \pmod{4284}$	5714857
64	$k \equiv 4123 \pmod{4284}$	$p_{4284,1}$
65	$k \equiv 1063 \pmod{3213}$	7812268926269851
66	$k \equiv 2134 \pmod{3213}$	$p_{3213,1}$
67	$k \equiv 3205 \pmod{3213}$	$p_{3213,1}$
68	$k \equiv 31 \pmod{85}$	108971
69	$k \equiv 36 \pmod{85}$	391206807721
70	$k \equiv 41 \pmod{85}$	21736504684553261
71	$k \equiv 46 \pmod{85}$	P_{85}
72	$k \equiv 51 \pmod{170}$	232122807601
73	$k \equiv 136 \pmod{170}$	P_{170}
74	$k \equiv 56 \pmod{255}$	934831
75	$k \equiv 141 \pmod{255}$	$p_{255,1}$
76	$k \equiv 226 \pmod{255}$	$p_{255,2}$
77	$k \equiv 61 \pmod{340}$	1361
78	$k \equiv 146 \pmod{340}$	3061
79	$k \equiv 231 \pmod{340}$	30941
80	$k \equiv 316 \pmod{340}$	2964461
81	$k \equiv 68 \pmod{340}$	5153381
82	$k \equiv 153 \pmod{340}$	$p_{340,1}$
83	$k \equiv 238 \pmod{340}$	$p_{340,2}$

row	congruence	prime p_i
84	$k \equiv 323 \pmod{680}$	3576121
85	$k \equiv 663 \pmod{680}$	$p_{680,1}$
86	$k \equiv 71 \pmod{765}$	1531
87	$k \equiv 156 \pmod{765}$	6121
88	$k \equiv 241 \pmod{765}$	1074061
89	$k \equiv 326 \pmod{765}$	8197741
90	$k \equiv 411 \pmod{765}$	$p_{765,1}$
91	$k \equiv 496 \pmod{765}$	$p_{765,2}$
92	$k \equiv 581 \pmod{1530}$	$p_{1530,1}$
93	$k \equiv 1346 \pmod{1530}$	$p_{1530,2}$
94	$k \equiv 666 \pmod{2295}$	4591
95	$k \equiv 1431 \pmod{2295}$	9181
96	$k \equiv 2196 \pmod{2295}$	59671
97	$k \equiv 751 \pmod{2295}$	$p_{2295,1}$
98	$k \equiv 1516 \pmod{2295}$	$p_{2295,2}$
99	$k \equiv 2281 \pmod{4590}$	2519911
100	$k \equiv 4576 \pmod{4590}$	$p_{4590,1}$
101	$k \equiv 76 \pmod{425}$	$p_{425,1}$
102	$k \equiv 161 \pmod{425}$	$p_{425,2}$
103	$k \equiv 246 \pmod{850}$	40801
104	$k \equiv 671 \pmod{850}$	$p_{850,1}$
105	$k \equiv 331 \pmod{850}$	$p_{850,2}$
106	$k \equiv 756 \pmod{1700}$	630701
107	$k \equiv 1606 \pmod{1700}$	865301

Table A.44 Fourth part of covering for $A + 18 \cdot 31^k$

row	congruence	prime p_i
108	$k \equiv 416 \pmod{1275}$	$p_{1275,1}$
109	$k \equiv 841 \pmod{1275}$	$p_{1275,2}$
110	$k \equiv 1266 \pmod{2550}$	2551
111	$k \equiv 2541 \pmod{2550}$	$p_{2550,1}$
112	$k \equiv 81 \pmod{595}$	89278561
113	$k \equiv 166 \pmod{595}$	108837401
114	$k \equiv 251 \pmod{595}$	42498121331
115	$k \equiv 336 \pmod{595}$	p_{115}
116	$k \equiv 421 \pmod{595}$	$p_{595,1}$
117	$k \equiv 506 \pmod{595}$	$p_{595,2}$
118	$k \equiv 591 \pmod{1190}$	2381
119	$k \equiv 1186 \pmod{1190}$	$p_{1190,1}$
120	$k \equiv 2 \pmod{5}$	11
121	$k \equiv 13 \pmod{16}$	17
122	$k \equiv 5 \pmod{64}$	4801
123	$k \equiv 21 \pmod{64}$	P_{64}
124	$k \equiv 37 \pmod{128}$	257
125	$k \equiv 101 \pmod{128}$	641
126	$k \equiv 53 \pmod{128}$	2689
127	$k \equiv 117 \pmod{128}$	9601
128	$k \equiv 3 \pmod{80}$	136046551681
129	$k \equiv 43 \pmod{80}$	p_{129}
130	$k \equiv 23 \pmod{160}$	380641
131	$k \equiv 103 \pmod{160}$	1176641

row	congruence	prime p_i
132	$k \equiv 33 \pmod{160}$	8084410241
133	$k \equiv 113 \pmod{320}$	259201
134	$k \equiv 273 \pmod{320}$	59826881
135	$k \equiv 63 \pmod{160}$	$p_{160,1}$
136	$k \equiv 143 \pmod{160}$	$p_{160,2}$
137	$k \equiv 73 \pmod{320}$	$p_{320,1}$
138	$k \equiv 233 \pmod{320}$	$p_{320,2}$
139	$k \equiv 153 \pmod{480}$	20641
140	$k \equiv 313 \pmod{480}$	$p_{480,1}$
141	$k \equiv 473 \pmod{480}$	$p_{480,2}$
142	$k \equiv 3 \pmod{45}$	337048683633480845467801
143	$k \equiv 8 \pmod{90}$	2065411
144	$k \equiv 53 \pmod{90}$	3003922640442496015027335982 51
145	$k \equiv 13 \pmod{135}$	1344742561
146	$k \equiv 58 \pmod{135}$	$p_{135,1}$
147	$k \equiv 103 \pmod{135}$	$p_{135,2}$
148	$k \equiv 24 \pmod{180}$	8728381
149	$k \equiv 84 \pmod{180}$	14398921
150	$k \equiv 144 \pmod{180}$	P_{180}
151	$k \equiv 29 \pmod{30}$	880374069121
152	$k \equiv 9 \pmod{60}$	61
153	$k \equiv 39 \pmod{60}$	25621
154	$k \equiv 19 \pmod{60}$	1529401
155	$k \equiv 49 \pmod{60}$	304643210761

For Tables A.45 and A.46, we set

$$p_{27} = 113917467341061919410563416404556311762533937215765064287981 1073,$$

$$p_{39} = 623224193931536278517290374646842636993833892690553820396 63,$$

$$p_{41} = 147882001432537751112306358052999119715341090542830827.$$

Table A.45 First part of covering for $A + 20 \cdot 31^k$

row	congruence	prime p_i
1	$k \equiv 5 \pmod 6$	7
2	$k \equiv 4 \pmod{16}$	17
3	$k \equiv 0 \pmod 7$	917087137
4	$k \equiv 1 \pmod{14}$	11971
5	$k \equiv 8 \pmod{14}$	71821
6	$k \equiv 2 \pmod{21}$	43
7	$k \equiv 9 \pmod{21}$	6301
8	$k \equiv 16 \pmod{21}$	2813432694367
9	$k \equiv 3 \pmod{28}$	29
10	$k \equiv 10 \pmod{28}$	7253
11	$k \equiv 17 \pmod{28}$	13469
12	$k \equiv 24 \pmod{28}$	277739477
13	$k \equiv 4 \pmod{35}$	319061
14	$k \equiv 11 \pmod{35}$	203633641
15	$k \equiv 18 \pmod{35}$	9240957640390889951861
16	$k \equiv 25 \pmod{70}$	71
17	$k \equiv 60 \pmod{70}$	149269961
18	$k \equiv 32 \pmod{70}$	60427990638165876546967231
19	$k \equiv 67 \pmod{140}$	281
20	$k \equiv 137 \pmod{140}$	106261
21	$k \equiv 5 \pmod{42}$	211
22	$k \equiv 12 \pmod{42}$	550469850411853
23	$k \equiv 19 \pmod{84}$	163598989
24	$k \equiv 61 \pmod{84}$	4038949965541
25	$k \equiv 26 \pmod{84}$	4038949965541
26	$k \equiv 68 \pmod{168}$	337886977
27	$k \equiv 152 \pmod{168}$	p_{27}
28	$k \equiv 33 \pmod{210}$	13454000701
29	$k \equiv 75 \pmod{210}$	18396393590821
30	$k \equiv 117 \pmod{210}$	350121327433921
31	$k \equiv 159 \pmod{210}$	430313436868714599746793868284888 1

Table A.46 Second part of covering for $A + 20 \cdot 31^k$

row	congruence	prime p_i
32	$k \equiv 201 \pmod{420}$	P_{420}
33	$k \equiv 411 \pmod{840}$	30241
34	$k \equiv 831 \pmod{840}$	52081
35	$k \equiv 40 \pmod{126}$	2143
36	$k \equiv 82 \pmod{126}$	45376431752737
37	$k \equiv 124 \pmod{126}$	1652484831253806817
38	$k \equiv 6 \pmod{49}$	6959
39	$k \equiv 13 \pmod{49}$	p_{39}
40	$k \equiv 20 \pmod{98}$	2932755253
41	$k \equiv 69 \pmod{98}$	p_{41}
42	$k \equiv 27 \pmod{147}$	883
43	$k \equiv 76 \pmod{147}$	$p_{147,1}$
44	$k \equiv 125 \pmod{147}$	$p_{147,2}$
45	$k \equiv 34 \pmod{196}$	197
46	$k \equiv 83 \pmod{196}$	P_{196}
47	$k \equiv 132 \pmod{392}$	29401
48	$k \equiv 328 \pmod{392}$	946681
49	$k \equiv 181 \pmod{392}$	$p_{392,1}$
50	$k \equiv 377 \pmod{392}$	$p_{392,2}$
51	$k \equiv 41 \pmod{245}$	491
52	$k \equiv 90 \pmod{245}$	55848731
53	$k \equiv 139 \pmod{245}$	$p_{245,1}$
54	$k \equiv 188 \pmod{245}$	$p_{245,2}$
55	$k \equiv 237 \pmod{490}$	1471
56	$k \equiv 482 \pmod{490}$	32341
57	$k \equiv 48 \pmod{294}$	159937
58	$k \equiv 97 \pmod{294}$	9561579721
59	$k \equiv 146 \pmod{294}$	64636178950385134849
60	$k \equiv 195 \pmod{588}$	$p_{588,1}$
61	$k \equiv 489 \pmod{588}$	$p_{588,2}$
62	$k \equiv 244 \pmod{882}$	154351
63	$k \equiv 538 \pmod{882}$	$p_{882,1}$
64	$k \equiv 832 \pmod{882}$	$p_{882,2}$
65	$k \equiv 293 \pmod{1470}$	282506071
66	$k \equiv 587 \pmod{1470}$	$p_{1470,1}$
67	$k \equiv 881 \pmod{1470}$	$p_{1470,2}$
68	$k \equiv 1175 \pmod{2940}$	126421
69	$k \equiv 2645 \pmod{2940}$	135241
70	$k \equiv 1469 \pmod{2940}$	840841
71	$k \equiv 2939 \pmod{2940}$	33183781

Appendix B

SageMath code

In this appendix we provide various SageMath programs and functions that were used to find primes where a given base has a given order, as well as to check whether primes were digitally delicate. We have broken the code into sections to provide additional structure.

B.1 Finding prime divisors of $\Phi_n(a)$

```
# Initialize polynomial ring R, order n, and base a.
# Calculate nth cyclotomic polynomial at a.
R = ZZ['x']
n=18 # Or the order you're looking for.
n
a=3 # Or the base you're covering.
f=R.cyclotomic_polynomial(n)(a)

# Check if largest prime divisor p of n divides f.
# If so, replace f by f/p.
# In each case, check if f is a prime power.
if n>1:
    p=max(n.prime_factors())
    if f%p!=0:
        f.is_prime_power()
```

```
    else:
        print("p divides.")
        f=Integer(f/p)
        f.is_prime_power()

# Search for small primes congruent to 1 mod n that divide f.
# Terminate if all primes found (primeprod==f).
# To look for more primes, change 10^7 to something larger.
primes=[]
primeprod=1
k=1
while primeprod<f and k<min(10^7,(f-1)/n+1):
    if f%(n*k+1)==0 and (n*k+1).is_prime():
        print(n*k+1)
        primes.append(n*k+1)
        primeprod=primeprod*(n*k+1)
    k=k+1

# Divide f by primes found above.
# Check if quotient is a prime power.
for prime in primes:
    f=Integer(f/prime)
    while gcd(f,prime)>1:
        f=Integer(f/prime)
        print(prime)
if f==1:
    print("No primes left.")
```

```
else:
    print(f)
    f.is_prime_power()
```

B.2 Checking whether primes are digitally delicate

```
def baserep(n,b):
    # Returns representation of integer in a particular base.
    # Input: Integers n, b.
    # Output: List representing n in base b.
    # Base case: n less than b.
    if n<b:
        return [n]
    # Recursive step: Peel off units digit, truncate n.
    else:
        return [n%b] + baserep((n-n%b)/b,b)

def digdelcheck(p, b):
    # Checks if an integer is digitally delicate in a given
       base.
    # Input: Integers p, b.
    # Output: Boolean boolvar.
    # Initialize return variable, express p in base b.
    boolvar=True
    pbaseb = baserep(p,b)

    # Initialize loop variables.
    i=0
```

```
    k=0
    # Iterate over all digit changes.
    while i!=len(pbaseb) and k!=b and boolvar:
        # Terminate if a prime is found.
        if (Integer(p + (k - pbaseb[i])*b^i).is_prime() or p
           + (k - pbaseb[i])*b^i==1) and Integer(p + (k -
           pbaseb[i])*b^i)!=p:
            print(p + (k - pbaseb[i])*b^i)
            boolvar=False
        # Increase digit/power as necessary.
        if k<b:
            k=k+1
        if k==b:
            if i<len(pbaseb):
                k=0
                i=i+1

    # Return conclusion.
    return boolvar

def widedigdelcheck(p,b,limit=100):
    # Checks if an integer is digitally delicate in a given
       base out to a specified number of leading zeros.
    # Input: Integers p, b, limit.
    # If no value is chosen for limit, program checks 100
       leading zeros.
    # Output: Boolean boolvar.
```

```
# Initialize return variable, express p in base b.
boolvar=True
pbaseb = baserep(p,b)

# Initialize loop variables.
i=0
k=0
# Iterate over all digit changes.
while i!=len(pbaseb) and k!=b and boolvar:
    # Terminate if a prime is found.
    if (Integer(p + (k - pbaseb[i])*b^i).is_prime() or p
       + (k - pbaseb[i])*b^i==1) and p + (k - pbaseb[i])*
       b^i!=p:
         boolvar=False
    # Increase digit/power as necessary.
    if k<b:
        k=k+1
    if k==b:
        if i<len(pbaseb):
            k=0
            i=i+1
# If p is digitally delicate, check leading zeros.
if boolvar:
    # Initialize loop variables. No longer need to
       consider delta = 0.
    i=len(pbaseb)+1
    k=1
```

```
        # Iterate over all digit changes.
        while i<len(pbaseb)+limit and k!=b and boolvar:
            # Terminate if a prime is found.
            if Integer(p + (k)*b^i).is_prime():
                boolvar=False
                #print(p+k*b^i, k, i)
            # Increase digit/power as necessary.
            if k<b:
                k=k+1
            if k==b:
                if i<len(pbaseb)+limit:
                    k=1
                    i=i+1
    # Return conclusion.
    return boolvar

def leadingzeroscheck(p,b,limit=100):
    # Checks whether leading zeros of an integer can be
       changed without obtaining a prime.
    # Input: Integers p, b, limit.
    # If no value is chosen for limit, program checks 100
       leading zeros.
    # Output: Boolean boolvar.
    # Initialize return variable, express p in base b.
    boolvar=True
    pbaseb = len(baserep(p,b))
```

```
    # Initialize loop variables.
    i=pbaseb+1
    k=1
    # Iterate over all possible digit changes.
    while i<pbaseb+limit and k!=b and boolvar:
        # Terminate if a prime is found.
        if Integer(p + (k)*b^i).is_prime():
            boolvar=False
            print(p+k*b^i, k, i)
        # Increase digit/power as necessary.
        if k<b:
            k=k+1
        if k==b:
            if i<pbaseb+limit:
                k=1
                i=i+1
    # Return conclusion.
    return boolvar
```

B.3 Checking whether a system of congruences is a covering

```
# List congruences k = a (mod m) in two lists.
# moduli is the list of m.
# kay is the list of congruence classes a.
moduli = [3, 6, 9, 18, 18, 4, 12, 36, 8, 72, 144, 144, 216,
   216, 216, 108, 216, 216]
kay = [0, 1, 2, 8, 14, 0, 10, 5, 3, 17, 53, 125, 23, 95, 167,
    71, 143, 215]
```

```
# Calculate least common multiple of moduli.
M = lcm(moduli)
M


# Create list of residues to check.
tocover = [i for i in range(M)]
# For each residue, check if some congruence covers the
   residue.
for j in range(len(moduli)):
    for k in set(tocover):
        if k%moduli[j]==kay[j]:
            tocover.remove(k)
# Display what is left to cover.
tocover
# Display percentage of residues left.
float(len(tocover)/M)
```